



**FORTINET**®



# FortiOS™ Handbook - FortiWiFi and FortiAP Configuration Guide

VERSION 6.0.2

**FORTIOS  
VERSION  
6.0**

## **FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

## **FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

## **FORTINET KNOWLEDGE BASE**

<http://kb.fortinet.com>

## **FORTINET BLOG**

<https://blog.fortinet.com>

## **CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

## **FORTINET COOKBOOK**

<http://cookbook.fortinet.com>

## **FORTINET TRAINING AND CERTIFICATION PROGRAM**

<https://www.fortinet.com/support-and-training/training.html>

## **NSE INSTITUTE**

<https://training.fortinet.com/>

## **FORTIGUARD CENTER**

<https://fortiguard.com>

## **FORTICAST**

<http://forticast.fortinet.com>

## **END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>



August 21, 2018

FortiOS™ Handbook - FortiWiFi and FortiAP Configuration Guide

01-602-481070-20180821

# TABLE OF CONTENTS

<b>Change log</b>	<b>9</b>
<b>Introduction</b>	<b>10</b>
Before you begin	10
How this guide is organized	10
What's new in FortiOS 6.0.1	11
What's new in FortiOS 6.0	11
<b>Introduction to wireless networking</b>	<b>12</b>
Wireless concepts	12
Bands and channels	12
Power	13
Antennas	13
Security	13
Whether to broadcast SSID	13
Encryption	13
Separate access for employees and guests	14
Captive portal	14
Power	14
Monitoring for rogue APs	14
Authentication	15
Wireless networking equipment	16
FortiWiFi units	16
FortiAP units	16
Automatic Radio Resource Provisioning	16
Setting ARRP timing	17
<b>Captive portals</b>	<b>18</b>
Introduction to captive portals	18
Configuring a captive portal	18
Exemption from the captive portal	20
MAC Bypass for captive portal	20
Customizing captive portal pages	21
Changing images in portal messages	24
Modifying text in portal messages	24
Configuring disclaimer page for ethernet interface captive portals	25
Roaming support	25

Session timeout interval for captive portal .....	25
Configuration example - captive portal WiFi access control .....	26
<b>Configuring a WiFi LAN .....</b>	<b>29</b>
Overview of WiFi controller configuration .....	30
About SSIDs on FortiWiFi units .....	31
Process to create a wireless network .....	31
Setting your geographic location .....	32
View all country and regcodes/regulatory domains .....	32
Creating a FortiAP profile .....	33
Defining a wireless network interface (SSID) .....	35
Configuring DHCP for WiFi clients .....	38
Configuring security .....	39
Adding a MAC filter .....	41
Limiting the number of clients .....	42
Multicast enhancement .....	43
Configuring WiFi captive portal security - FortiGate captive portal .....	43
Configuring WiFi captive portal security - external server .....	43
Defining SSID groups .....	44
Dynamic user VLAN assignment .....	45
VLAN assignment by RADIUS .....	45
VLAN assignment by VLAN pool .....	47
Configuring user authentication .....	48
WPA2 Enterprise authentication .....	48
WiFi single sign-on (WSSO) authentication .....	49
Assigning WiFi users to VLANs dynamically .....	50
MAC-based authentication .....	50
Authenticating guest WiFi users .....	50
Configuring firewall policies for the SSID .....	51
Configuring the built-in access point on a FortiWiFi unit .....	52
Enforcing UTM policies on a local bridge SSID for managed smart APs .....	52
<b>Access point deployment .....</b>	<b>54</b>
Overview .....	54
Network topology for managed APs .....	54
Discovering and authorizing APs .....	58
Configuring the network interface for the AP unit .....	59
Pre-authorizing a FortiAP unit .....	59
Enabling and configuring a discovered AP .....	60
Disable automatic discovery of unknown FortiAPs .....	61
Automatic authorization of extension devices .....	61
Assigning the same profile to multiple FortiAP units .....	61
Overriding the FortiAP profile .....	61
Accessing the FortiAP CLI through the FortiGate unit .....	62

Connecting to the FortiAP CLI.....	62
Checking and updating FortiAP unit firmware.....	63
Advanced WiFi controller discovery.....	65
Controller discovery methods.....	65
Wireless client load balancing for high-density deployments.....	67
Access point hand-off.....	67
Frequency hand-off or band-steering.....	67
Configuration.....	67
FortiAP groups.....	68
LAN port options.....	68
Bridging a LAN port with an SSID.....	69
Bridging a LAN port with the WAN port.....	69
Configuring FortiAP LAN ports.....	70
Preventing IP fragmentation of packets in CAPWAP tunnels.....	71
Overriding IP fragmentation settings on a FortiAP.....	72
LED options.....	72
CAPWAP bandwidth formula.....	73
Enabling LLDP protocol.....	75
<b>Wireless mesh.....</b>	<b>76</b>
Overview of wireless mesh.....	76
Wireless mesh deployment modes.....	77
Firmware requirements.....	77
Types of wireless mesh.....	77
Fast-roaming for mesh backhaul link.....	78
Configuring a meshed WiFi network.....	79
Creating the mesh root SSID.....	79
Creating the FortiAP profile.....	79
Configuring the mesh root AP.....	79
Configuring the mesh leaf FortiAPs.....	80
Authorizing leaf APs.....	81
Creating security policies.....	81
Viewing the status of the mesh network.....	82
Configuring a point-to-point bridge.....	82
<b>Hotspot 2.0.....</b>	<b>84</b>
<b>Combining WiFi and wired networks with a software switch.....</b>	<b>88</b>
Combining WiFi and wired networks with a software switch.....	88
VLAN configuration.....	90
Additional configuration.....	90
FortiAP local bridging (Private cloud-managed AP).....	90
Continued FortiAP operation when WiFi controller connection is down.....	93
Using bridged FortiAPs to increase scalability.....	93
<b>Using remote WLAN FortiAPs.....</b>	<b>95</b>

Split tunneling.....	95
Configuring the FortiGate for remote FortiAPs.....	95
Override Split tunneling.....	95
Creating FortiAP profiles.....	95
Configuring split tunneling - FortiGate GUI.....	96
Configuring split tunneling - FortiGate CLI.....	96
Overriding the split tunneling settings on a FortiAP.....	96
Configuring the FortiAP units.....	97
Preauthorizing FortiAP units.....	97
<b>Features for high-density deployments.....</b>	<b>98</b>
Multiple FortiAP firmware upgrades at once.....	98
Power save feature.....	98
Broadcast packet suppression.....	99
Multicast to unicast conversion.....	100
Ignore weak or distant clients.....	100
Turn off the 802.11b protocol.....	101
Disable low data rates.....	101
Limit power.....	101
Use frequency band load-balancing.....	102
Setting the handoff RSSI threshold.....	102
AP load balancing.....	102
Setting the AP load balance threshold.....	103
Application rate-limiting.....	103
AP group management and dynamic VLAN assignment.....	103
Sharing tunnel SSIDs within a single managed AP between VDOMs as a virtual AP for multi-tenancy.....	104
Manual quarantine of devices on FortiAP (tunnel mode).....	104
Host quarantine per SSID.....	105
Locate a FortiAP with LED blinking.....	105
Wireless controller optimization for large deployment - AP image upgrade.....	106
Control message off-loading and aeroscout enhancement.....	106
<b>Protecting the WiFi network.....</b>	<b>108</b>
Wireless IDS.....	108
Rogue AP detection.....	109
WIDS client deauthentication rate for DoS attacks.....	109
WiFi data channel encryption.....	109
Configuring encryption on the FortiGate unit.....	109
Configuring encryption on the FortiAP unit.....	110
Protected Management Frames and Opportunistic Key Caching support.....	110
Bluetooth Low Energy (BLE) Scan.....	111
Preventing local bridge traffic from reaching the LAN.....	112
FortiAP-S bridge mode security profiles.....	112

DHCP snooping and option 82 (circuit-id) options for wireless access points.....	113
<b>Wireless network monitoring.....</b>	<b>114</b>
Monitoring wireless clients.....	114
Monitoring rogue APs.....	114
On-wire rogue AP detection technique.....	115
Rogue AP scanning as a background activity.....	115
Configuring rogue scanning.....	116
Using the Rogue AP Monitor.....	118
Suppressing rogue APs.....	119
Monitoring wireless network health.....	119
<b>Configuring wireless network clients.....</b>	<b>121</b>
Windows XP client.....	121
Windows 7 client.....	126
Mac OS client.....	130
Linux client.....	132
Troubleshooting.....	134
Checking that client received IP address and DNS server information.....	134
<b>Wireless network examples.....</b>	<b>137</b>
Basic wireless network.....	137
Configuring authentication for wireless users.....	137
Configuring the SSID.....	138
Adding the SSID to the FortiAP Profile.....	139
Configuring security policies.....	139
Connecting the FortiAP units.....	140
A more complex example.....	142
Scenario.....	142
Configuration.....	142
Configuring authentication for employee wireless users.....	143
Configuring authentication for guest wireless users.....	143
Configuring the SSIDs.....	145
Configuring the FortiAP profile.....	147
Configuring firewall policies.....	148
Connecting the FortiAP units.....	150
<b>Managing a FortiAP with FortiCloud.....</b>	<b>152</b>
FortiCloud-managed FortiAP WiFi.....	152
Adding your FortiAP to FortiCloud.....	152
Configuring the SSID.....	152
Configuring the AP platform profile.....	153
Deploying the AP with the platform profile.....	153
FortiCloud-managed FortiAP WiFi without a key.....	153
Configuring the FortiAP unit.....	154
Adding the FortiAP unit to your FortiCloud account.....	154

<b>Using a FortiWiFi unit as a client</b>	<b>155</b>
Use of client mode	155
Configuring client mode	157
Controlled AP selection support in FWF client mode	158
<b>Support for location-based services</b>	<b>159</b>
Overview	159
Configuring location tracking	159
Automatic deletion of outdated presence data	159
FortiPresence push REST API	160
Viewing device location data on the FortiGate unit	160
<b>Troubleshooting</b>	<b>162</b>
FortiAP shell command through CAPWAP control tunnel	162
Signal strength issues	163
Asymmetric power issue	163
Frequency interference	165
Throughput issues	166
Testing the link	166
Performance testing	167
Preventing IP fragmentation in CAPWAP	168
Slowness in the DTLS response	168
Connection issues	168
Client connection issues	168
FortiAP connection issues	170
General problems	173
Best practices for Layer 1	174
Best practices for Layer 2	174
Best practices for Layer 3 and above	175
Packet sniffer	176
CAPWAP packet sniffer	176
Wireless traffic packet sniffer	177
Useful debugging commands	179
Sample outputs	180
Support for extension information for wtp, vap, and station	180
<b>Reference</b>	<b>181</b>
FortiAP web-based manager	182
System information	182
Wireless information	183
Wireless radio channels	184
IEEE 802.11a/n channels	184
View all country and regcodes/regulatory domains	185
WiFi event types	186
FortiAP CLI	186



# Change log

Date	Change description
August 21, 2018	Clarification of the CLI options in discussion of <a href="#">"Broadcast packet suppression" on page 99</a> . Added information to <a href="#">"Configuring a meshed WiFi network" on page 79</a> and to <a href="#">"Configuring a point-to-point bridge" on page 82</a> .
June 5, 2018	FortiOS 6.0.1 document release. See <a href="#">"What's new in FortiOS 6.0.1" on page 11</a> .
March 29, 2018	FortiOS 6.0 document release. See <a href="#">"What's new in FortiOS 6.0" on page 11</a> .

# Introduction

Welcome and thank you for selecting Fortinet products for your network protection. This document describes how to configure wireless networks with FortiWiFi, FortiGate, and FortiAP devices.

This chapter contains the following topics:

- [Before you begin](#)
- [How this guide is organized](#)

## Before you begin

Before you begin using this guide, please ensure that:

- You have administrative access to the FortiGate GUI and/or CLI.
- The FortiGate is integrated into your network.
- The operation mode has been configured.
- The system time, DNS settings, administrator password, and network interfaces have been configured.
- Firmware, FortiGuard Antivirus, and FortiGuard Antispam are up to date.
- FortiGuard Analysis & Management Service is properly configured.

While using the instructions in this guide, note that administrators are assumed to be super\_admin administrators unless otherwise specified. Some restrictions will apply to other administrators.

## How this guide is organized

This FortiOS Handbook chapter contains the following sections:

[Introduction to wireless networking](#) explains the basic concepts of wireless networking and how to plan your wireless network.

[Configuring a WiFi LAN](#) explains how to set up a basic wireless network, prior to deploying access point hardware.

[Access point deployment](#) explains how to deploy access point hardware and add it to your wireless network configuration.

[Wireless mesh](#) explains how to configure a Wi-Fi network where access points are connected to the Wi-Fi controller wirelessly instead of by Ethernet.

[Combining WiFi and wired networks with a software switch](#) shows how to use the FortiAP Wi-Fi-Ethernet bridge feature.

[Protecting the WiFi network](#) explains the Wireless Intrusion Detection System (WIDS).

[Wireless network monitoring](#) explains how to monitor your wireless clients and how to monitor other wireless access points, potentially rogues, in your coverage area.

[Configuring wireless network clients](#) explains how to configure typical wireless clients to work with a WPA-Enterprise protected network.

[Wireless network examples](#) provides two examples. The first is a simple Wi-Fi network using automatic configuration. The second is a more complex example of a business with two Wi-Fi networks, one for employees and another for guests or customers.

[Using a FortiWiFi unit as a client](#) explains how to use a FortiWiFi unit as a wireless client to connect to other Wi-Fi networks. This connection can take the place of an Ethernet connection where wired access to a network or to the Internet is not available.

[Support for location-based services](#) explains how Fortinet supports location-based services that collect information about devices near FortiGate-managed access points, even if the devices don't associate with the network.

[Reference](#) provides information about Wi-Fi radio channels.

## What's new in FortiOS 6.0.1

The following new wireless features added in FortiOS 6.0.1. Click on a link to navigate to that section for further information.

- ["Locate a FortiAP with LED blinking" on page 105](#)

## What's new in FortiOS 6.0

The following list contains new wireless features added in FortiOS 6.0. Click on a link to navigate to that section for further information.

- ["MAC-auth-bypass for the captive-portal SSID" on page 20](#)
- ["Session timeout interval for captive portal" on page 25](#)
- ["Enforcing UTM policies on a local bridge SSID for managed smart APs" on page 52](#)
- ["Multiple FortiAP firmware upgrades at once" on page 98](#)
- ["Manual quarantine of devices on FortiAP \(tunnel mode\)" on page 104](#)
- ["Host quarantine per SSID" on page 105](#)
- ["Locate a FortiAP with LED blinking" on page 105](#)
- ["Wireless controller optimization for large deployment - AP image upgrade" on page 106](#)
- ["Control message off-loading and aeroscout enhancement" on page 106](#)
- ["Preventing local bridge traffic from reaching the LAN" on page 112](#)
- ["FortiAP-S bridge mode security profiles" on page 112](#)
- ["DHCP snooping and option 82 \(circuit -id\) options for wireless access points" on page 113](#)
- ["WiFi Channel Utilization" on page 120](#)
- ["Support for extension information for wtp, vap, and station" on page 180](#)

# Introduction to wireless networking

This chapter introduces some concepts you should understand before working with wireless networks, describes Fortinet's wireless equipment, and then describes the factors you need to consider in planning deployment of a wireless network.

Wireless concepts

Security

Authentication

Wireless networking equipment

Automatic Radio Resource Provisioning

## Wireless concepts

Wireless networking is radio technology, subject to the same characteristics and limitations as the familiar audio and video radio communications. Various techniques are used to modulate the radio signal with a data stream.

## Bands and channels

Depending on the wireless protocol selected, you have specific channels available to you, depending on what region of the world you are in.

- IEEE 802.11b and g protocols provide up to 14 channels in the 2.400-2.500 GHz Industrial, Scientific and Medical (ISM) band.
- IEEE 802.11a,n (5.150-5.250, 5.250-5.350, 5.725–5.875 GHz, up to 16 channels) in portions of Unlicensed National Information Infrastructure (U-NII) band

Note that the width of these channels exceeds the spacing between the channels. This means that there is some overlap, creating the possibility of interference from adjacent channels, although less severe than interference on the same channel. Truly non-overlapping operation requires the use of every fourth or fifth channel, for example ISM channels 1, 6 and 11.

The capabilities of your wireless clients is the deciding factor in your choice of wireless protocol. If your clients support it, 5GHz protocols have some advantages. The 5GHz band is less used than 2.4GHz and its shorter wavelengths have a shorter range and penetrate obstacles less. All of these factors mean less interference from other access points, including your own.

When configuring your WAP, be sure to correctly select the Geography setting to ensure that you have access only to the channels permitted for WiFi use in your part of the world.

For detailed information about the channel assignments for wireless networks for each supported wireless protocol, see [Reference on page 181](#).

## Power

Wireless LANs operate on frequencies that require no license but are limited by regulations to low power. As with other unlicensed radio operations, the regulations provide no protection against interference from other users who are in compliance with the regulations.

Power is often quoted in dBm. This is the power level in decibels compared to one milliwatt. 0dBm is one milliwatt, 10dBm is 10 milliwatts, 27dBm, the maximum power on Fortinet FortiAP equipment, is 500 milliwatts. The FortiGate unit limits the actual power available to the maximum permitted in your region as selected by the WiFi controller country setting.

Received signal strength is almost always quoted in dBm because the received power is very small. The numbers are negative because they are less than the one milliwatt reference. A received signal strength of -60dBm is one millionth of a milliwatt or one nanowatt.

## Antennas

Transmitted signal strength is a function of transmitter power and antenna gain. Directional antennas concentrate the signal in one direction, providing a stronger signal in that direction than would an omnidirectional antenna.

FortiWiFi units have detachable antennas. However, these units receive regulatory approvals based on the supplied antenna. Changing the antenna might cause your unit to violate radio regulations.

## Security

There are several security issues to consider when setting up a wireless network.

### Whether to broadcast SSID

It is highly recommended to broadcast the SSID. This makes connection to a wireless network easier because most wireless client applications present the user with a list of network SSIDs currently being received. This is desirable for a public network.

Attempting to obscure the presence of a wireless network by not broadcasting the SSID does not improve network security. The network is still detectable with wireless network “sniffer” software. Clients search for SSIDs that they know, leaking the SSID. Refer to [RFC 3370](#). Also, many of the latest Broadcom drivers do not support hidden SSID for WPA2.

## Encryption

Wireless networking supports the following security modes for protecting wireless communication, listed in order of increasing security.

**None** — Open system. Any wireless user can connect to the wireless network.

**WEP64** — 64-bit Web Equivalent Privacy (WEP). This encryption requires a key containing 10 hexadecimal digits.

**WEP128** — 128-bit WEP. This encryption requires a key containing 26 hexadecimal digits.

**WPA** — 256-bit WiFi Protected Access (WPA) security. This encryption can use either the TKIP or AES encryption algorithm and requires a key of either 64 hexadecimal digits or a text phrase of 8 to 63 characters. It is also possible to use a RADIUS server to store a separate key for each user.

**WPA2** — WPA with security improvements fully meeting the requirements of the IEEE 802.11i standard. Configuration requirements are the same as for WPA.

For best security, use the WPA2 with AES encryption and a RADIUS server to verify individual credentials for each user. WEP, while better than no security at all, is an older algorithm that is easily compromised. With either WEP or WAP, changing encryption passphrases on a regular basis further enhances security.

## Separate access for employees and guests

Wireless access for guests or customers should be separate from wireless access for your employees. Each of the two networks can have its own SSID, security settings, firewall policies, and user authentication. This does not require additional hardware. Both FortiWiFi units and FortiAP units support multiple wireless LANs on the same access point.

A good practice is to broadcast the SSID for the guest network to make it easily visible to users, but not to broadcast the SSID for the employee network.

Two separate wireless networks are possible because multiple virtual APs can be associated with an AP profile. The same physical APs can provide two or more virtual WLANs.

## Captive portal

As part of authenticating your users, you might want them to view a web page containing your acceptable use policy or other information. This is called a captive portal. No matter what URL the user initially requested, the portal page is returned. Only after authenticating and agreeing to usage terms can the user access other web resources.

For more information about captive portals, see the Captive portals chapter of the FortiOS Authentication Guide.

## Power

Reducing power reduces unwanted coverage and potential interference to other WLANs. Areas of unwanted coverage are a potential security risk. There are people who look for wireless networks and attempt to access them. If your office WLAN is receivable out on the public street, you have created an opportunity for this sort of activity.

## Monitoring for rogue APs

It is likely that there are APs available in your location that are not part of your network. Most of these APs belong to neighboring businesses or homes. They may cause some interference, but they are not a security threat. There is a risk that people in your organization could connect unsecured WiFi-equipped devices to your wired network, inadvertently providing access to unauthorized parties. The optional On-Wire Rogue AP Detection Technique compares MAC addresses in the traffic of suspected rogues with the MAC addresses on your network. If wireless traffic to non-Fortinet APs is also seen on the wired network, the AP is a rogue, not an unrelated AP.

Decisions about which APs are rogues are made manually on the Rogue AP monitor page. For detailed information, see [Wireless network monitoring on page 114](#).

## Suppressing rogue APs

When you have declared an AP to be a rogue, you have the option of suppressing it. To suppress an AP, the FortiGate WiFi controller sends reset packets to the rogue AP. Also, the MAC address of the rogue AP is blocked in the firewall policy. You select the suppression action on the Rogue AP monitor page. For more information, see [Wireless network monitoring on page 114](#).



Rogue suppression is available only when there is a radio dedicated to scanning. It will not function during background scanning for spectrum analysis.

## Wireless Intrusion Detection (WIDS)

You can create a WIDS profile to enable several types of intrusion detection:

- Unauthorized Device Detection
- Rogue/Interfering AP Detection
- Ad-hoc Network Detection and Containment
- Wireless Bridge Detection
- Misconfigured AP Detection
- Weak WEP Detection
- Multi Tenancy Protection
- MAC OUI Checking

For more information, see [Protecting the WiFi network on page 108](#).

## Authentication

Wireless networks usually require authenticated access. FortiOS authentication methods apply to wireless networks the same as they do to wired networks because authentication is applied in the firewall policy.

The types of authentication that you might consider include:

- user accounts stored on the FortiGate
- user accounts managed and verified on an external RADIUS, LDAP or TACACS+ server
- Windows Active Directory authentication, in which users logged on to a Windows network are transparently authenticated to use the wireless network.

This FortiWiFi and FortiAP Configuration Guide provides some information about each type of authentication, but more detailed information is available in the Authentication chapter of the FortiOS Handbook.

What all of these types of authentication have in common is the definition of user groups to specify who is authorized. For each wireless LAN, you will create a user group and add to it the users who can use the WLAN. In the identity-based firewall policies that you create for your wireless LAN, you will specify this user group.

Some access points, including FortiWiFi units, support MAC address filtering. You should not rely on this alone for authentication. MAC addresses can be “sniffed” from wireless traffic and used to impersonate legitimate clients.

## Wireless networking equipment

Fortinet produces two types of wireless networking equipment:

- **FortiWiFi units**, which are FortiGate units with a built-in wireless access point/client
- **FortiAP units**, which are wireless access points that you can control from any FortiGate unit that supports the WiFi Controller feature.

### FortiWiFi units

A FortiWiFi unit can:

- Provide an access point for clients with wireless network cards. This is called Access Point mode, which is the default mode.  
**or**
- Connect the FortiWiFi unit to another wireless network. This is called Client mode. A FortiWiFi unit operating in client mode can only have one wireless interface.  
**or**
- Monitor access points within radio range. This is called Monitoring mode. You can designate the detected access points as Accepted or Rogue for tracking purposes. No access point or client operation is possible in this mode. But, you can enable monitoring as a background activity while the unit is in Access Point mode.

The Products section of the Fortinet web site ([www.fortinet.com](http://www.fortinet.com)) provides detailed information about the FortiWiFi models that are currently available.

### FortiAP units

FortiAP units are thin wireless access points are controlled by either a FortiGate unit or FortiCloud service.

FortiAP is a family of Indoor, Outdoor and Remote Access Point models supporting the latest single, dual, and triple stream MIMO 802.11ac and 802.11n technology, as well as 802.11g and 802.11a.

For large deployments, some FortiAP models support a mesh mode of operation in which control and data backhaul traffic between APs and the controller are carried on a dedicated WiFi network. Users can roam seamlessly from one AP to another.

In dual-radio models, each radio can function as an AP or as a dedicated monitor. The monitoring function is also available during AP operation, subject to traffic levels.

The [Products](#) section of the Fortinet web site ([www.fortinet.com](http://www.fortinet.com)) provides detailed information about the FortiAP models that are currently available.

## Automatic Radio Resource Provisioning

To prevent interference between APs, the FortiOS WiFi Controller includes the Distributed Automatic Radio Resource Provisioning (DARRP) feature. Through DARRP, each FortiAP unit autonomously and periodically determines the channel that is best suited for wireless communications. FortiAP units to select their channel so



that they do not interfere with each other in large-scale deployments where multiple access points have overlapping radio ranges.

### To enable ARRP - GUI

1. Go to **WiFi Controller > FortiAP Profiles** and edit the profile for your device.
2. In the Radio sections (Radio 1, Radio 2, etc.), enable **Radio Resource Provision**.
3. Click **OK**.

### To enable ARRP - CLI

In this example, ARRP is enabled for both radios in the FAP321C-default profile:

```
config wireless-controller wtp-profile
  edit FAP321C-default
    config radio-1
      set darrp enable
    end
    config radio-2
      set darrp enable
    end
  end
```

## Setting ARRP timing

By default, ARRP optimization occurs at a fixed interval of 1800 seconds (30 minutes). You can change this interval in the CLI. For example, to change the interval to 3600 seconds enter:

```
config wireless-controller timers
  set darrp-optimize 3600
end
```

Optionally, you can schedule optimization for fixed times. This enables you to confine ARRP activity to a low-traffic period. Setting `darrp-optimize` to 0, makes `darrp-day` and `darrp-time` available. For example, here's how to set DARRP optimization for 3:00am every day:

```
config wireless-controller timers
  set darrp-optimize 0
  set darrp-day sunday monday tuesday wednesday thursday friday saturday
  set darrp-time 03:00
end
```

Both `darrp-day` and `darrp-time` can accept multiple entries.

# Captive portals

A captive portal is a convenient way to authenticate web users on wired or WiFi networks.

This section describes:

- [Introduction to captive portals](#)
- [Configuring a captive portal](#)
- [Customizing captive portal pages](#)
- [Configuration example - captive portal WiFi access control](#)

## Introduction to captive portals

You can authenticate your users on a web page that requests the user's name and password. Until the user authenticates successfully, the authentication page is returned in response to any HTTP request. This is called a captive portal.

After successful authentication, the user accesses the requested URL and can access other web resources, as permitted by security policies. Optionally, the captive portal itself can allow web access to only the members of specified user group.

The captive portal can be hosted on the FortiGate unit or on an external authentication server. You can configure captive portal authentication on any network interface, including WiFi and VLAN interfaces.

When a captive portal is configured on a WiFi interface, the access point initially appears open. The wireless client can connect to the access point with no security credentials, but sees only the captive portal authentication page.

WiFi captive portal types:

- **Authentication** — until the user enters valid credentials, no communication beyond the AP is permitted.
- **Disclaimer + Authentication** — immediately after successful authentication, the portal presents the disclaimer page—an acceptable use policy or other legal statement—to which the user must agree before proceeding.
- **Disclaimer Only** — the portal presents the disclaimer page—an acceptable use policy or other legal statement—to which the user must agree before proceeding. The authentication page is not presented.
- **Email Collection** — the portal presents a page requesting the user's email address, for the purpose of contacting the person in future. This is often used by businesses who provide free WiFi access to their customers. The authentication page is not presented.
- **MAC Bypass** — when clients are authenticated against their bridged SSID and their MAC addresses are known, they are redirected to the external captive portal.

## Configuring a captive portal

Captive portals are configured on network interfaces. A WiFi interface does not exist until the WiFi SSID is created. You can configure a WiFi captive portal at the time that you create the SSID. Afterwards, the captive portal settings will also be available by editing the WiFi network interface in **System > Network > Interfaces**.

On a physical (wired) network interface, you edit the interface configuration in **System > Network > Interfaces** and set **Security Mode** to **Captive Portal**.

#### To configure a WiFi captive portal - web-based manager:

1. Go to **WiFi & Switch Controller > SSID** and create your SSID.  
If the SSID already exists, you can edit the SSID or you can edit the WiFi interface in **Network > Interfaces**.
2. Under **WiFi Settings**, for **Security Mode**, select **Captive Portal**.

WiFi Settings

SSID

fortinet

Security Mode

Captive Portal

Client Limit

☐

Portal Type

Authentication

Disclaimer + Authentication

Disclaimer Only

Email Collection

Authentication Portal

Local

External

example.com/captive/

User Groups

+

Exempt Sources

+

Exempt Destinations/Services

+

Redirect after Captive Portal

Original Request

Specific URL

3. Enter the following:

<b>Portal Type</b>	The portal can provide authentication and/or disclaimer, or perform user email address collection. See <a href="#">Introduction to captive portals on page 18</a> .
<b>Authentication Portal</b>	Local - portal hosted on the FortiGate unit.  Remote - enter FQDN or IP address of external portal.
<b>User Groups</b>	Select permitted user groups.
<b>Exempt Sources</b> <b>Exempt Destinations/Services</b>	Select exempt lists whose members will not be subject to captive portal authentication.
<b>Redirect after Captive Portal</b>	Select whether to have authenticated users navigate to their originally requested URL or be redirected to another/specific URL.

4. Select **OK**.

#### To configure an SSID with external-web enabled - CLI:

```
config wireless-controller vap
edit "web-ext"
set vdom "root"
set ssid "web-ext"
set security captive-portal
set selected-usergroups "qnap"
```

```

    set security-exempt-list "wifi"
    set security-redirect-url " http://www.fortinet.com"
    set intra-vap-privacy enable
    set local-switching disable
    set external-web "192.168.234.51/portal.php"
  next
end

```

Note that the `external-web` entry is the URL of the external authentication web server. When this entry is not set, the FortiGate will use the local web server hosting the local login/splash page.

The external web URL is not explicitly set with HTTP/HTTPS - FortiGate uses the `auth-secure-http` entry under `config user` setting.

## Exemption from the captive portal

A captive portal requires all users on the interface to authenticate. But some devices are not able to authenticate. You can create an exemption list of these devices. For example, a printer might need to access the Internet for firmware upgrades. Using the CLI, you can create an exemption list to exempt all printers from authentication.

```

config user security-exempt-list
  edit r_exempt
    config rule
      edit <id>
        set devices printer
      end
    end
  end
end

```

Furthermore, a walled garden firewall policy can be created:

```

config firewall policy
  edit <id>
    set captive-portal-exempt enable
    ...
  next
end

```

## MAC Bypass for captive portal

It is possible to provide a MAC address bypass for authenticated clients. When clients are authenticated with bridged SSID and their MAC addresses are known, they are redirected to the External Captive Portal.

A new portal type has been added, under `config wireless-controller vap`, to provide successful MAC authentication Captive Portal functionality.

### Syntax

```

config wireless-controller vap
  edit {name}
    set portal-type {cmcc-macauth}
  next
end

```

## MAC-auth-bypass for the captive-portal SSID

Captive-portal SSID supports MAC-auth-bypass. If a client's MAC can be authenticated from local-user or RADIUS, then the client can bypass firewall authentication directly.

```
config wireless-controller vap
  edit <name>
    set security captive-portal
    set MAC-auth-bypass {enable | disable}
  next
end
```

## Customizing captive portal pages

These pages are defined in replacement messages. Defaults are provided. In the web-based manager, you can modify the default messages in the SSID configuration by selecting **Customize Portal Messages**. Each SSID can have its own unique portal content.

The captive portal contains the following default web pages:

- **Login page**—requests user credentials

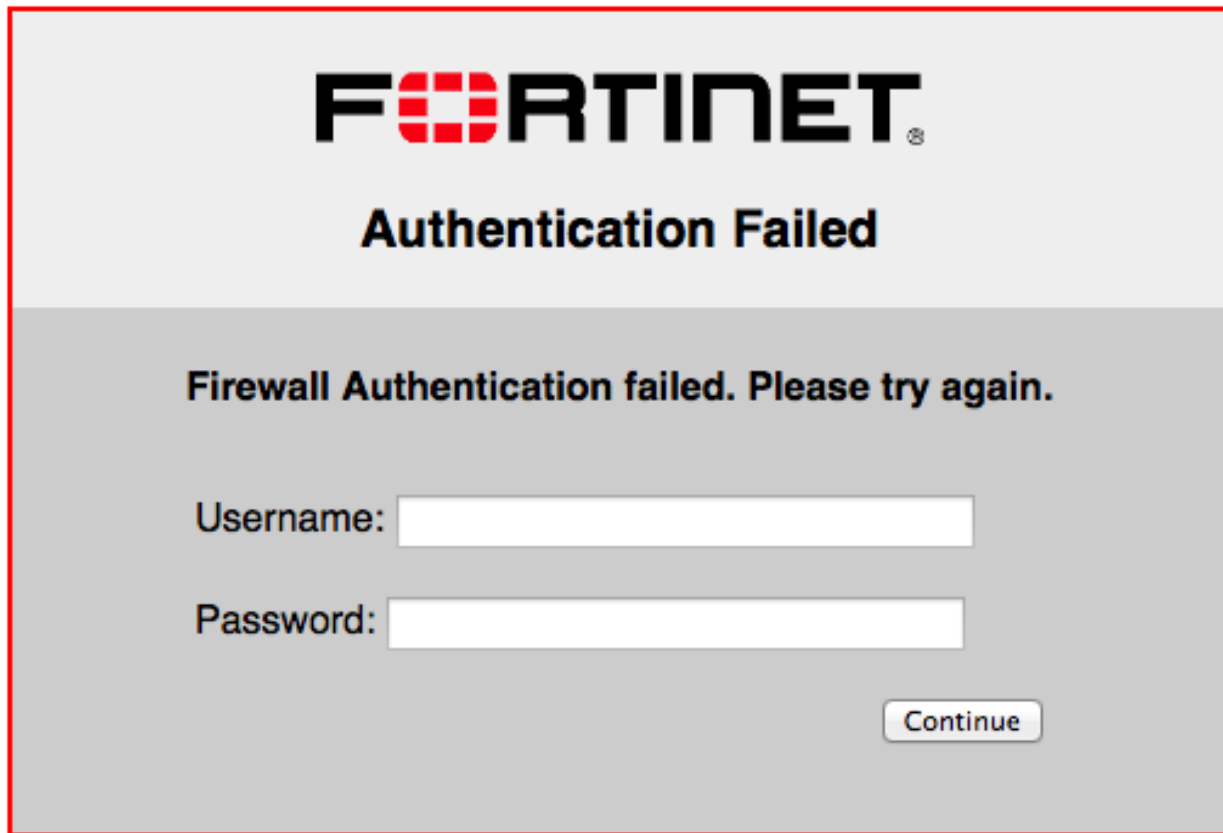
The image shows a captive portal login page for Fortinet. It has a light gray background with a red border. At the top, the Fortinet logo is displayed in black and red. Below the logo, the text "Authentication Required" is written in bold black font. Further down, the instruction "Please enter your credentials to continue." is shown in bold black font. There are two input fields: "Username:" followed by a white text box, and "Password:" followed by a white text box. At the bottom right, there is a "Continue" button with a gray gradient and a white border.

Typical modifications for this page would be to change the logo and modify some of the text.

You can change any text that is not part of the HTML code nor a special tag enclosed in double percent (%) characters.

There is an exception to this rule. The line "Please enter your credentials to continue" is provided by the `%%QUESTION%%` tag. You can replace this tag with text of your choice. Except for this item, you should not remove any tags because they may carry information that the FortiGate unit needs.

- **Login failed page**—reports that the entered credentials were incorrect and enables the user to try again.



The Login failed page is similar to the Login page. It even contains the same login form. You can change any text that is not part of the HTML code nor a special tag enclosed in double percent (%) characters.

There is an exception to this rule. The line “Firewall authentication failed. Please try again.” is provided by the %%FAILED\_MESSAGE%% tag. You can replace this tag with text of your choice. Except for this item, you should not remove any tags because they may carry information that the FortiGate unit needs.

- **Disclaimer page**—is a statement of the legal responsibilities of the user and the host organization to which the user must agree before proceeding. (WiFi or SSL VPN only)

## Terms and Disclaimer Agreement

You are about to access Internet content that is not under the control of the network access provider. The network access provider is therefore not responsible for any of these sites, their content or their privacy policies. The network access provider and its staff do not endorse nor make any representations about these sites, or any information, software or other products or materials found there, or any results that may be obtained from using them. If you decide to access any Internet content, you do this entirely at your own risk and you are responsible for ensuring that any accessed material does not infringe the laws governing, but not exhaustively covering, copyright, trademarks, pornography, or any other material which is slanderous, defamatory or might cause offence in any other way.

**Do you agree to the above terms?**

Yes, I agree

No, I decline

- **Declined disclaimer page**—is displayed if the user does not agree to the statement on the Disclaimer page. Access is denied until the user agrees to the disclaimer.

**FORTINET®**

### Disclaimer Declined

Sorry, network access cannot be granted unless you agree to the disclaimer.

Return to Disclaimer

## Changing images in portal messages

You can replace the default Fortinet logo with your organization's logo. First, import the logo file into the FortiGate unit and then modify the Login page code to reference your file.

### To import a logo file:

1. Go to **System > Replacement Messages** and select **Manage Images**.
2. Select **Create New**.
3. Enter a **Name** for the logo and select the appropriate **Content Type**.  
The file must not exceed 24 Kilo bytes.
4. Select **Browse**, find your logo file and then select **Open**.
5. Select **OK**.

### To specify the new logo in the replacement message:

1. Go to **Network > Interfaces** and edit the interface.  
The **Security Mode** must be **Captive Portal**.
2. Select the portal message to edit.
  - In SSL VPN or WiFi interfaces, in **Customize Portal Messages** click the link to the portal messages that you want to edit.
  - In other interfaces, make sure that **Customize Portal Messages** is selected, select the adjacent **Edit** icon, then select the message that you want to edit.
3. In the HTML message text, find the %%IMAGE tag.  
By default it specifies the Fortinet logo: %%IMAGE:logo\_fw\_auth%%
4. Change the image name to the one you provided for your logo.  
The tag should now read, for example, %%IMAGE:mylogo%%
5. Select **Save**.
6. Select **OK**.

## Modifying text in portal messages

Generally, you can change any text that is not part of the HTML code nor a special tag enclosed in double percent (%) characters. You should not remove any tags because they may carry information that the FortiGate unit needs. See the preceding section for any exceptions to this rule for particular pages.

### To modify portal page text

1. Go to **System > Network > Interfaces** and edit the interface.  
The SSID **Security Mode** must be **Captive Portal**.
2. Select the portal message to edit.
  - In SSL VPN or WiFi interfaces, in **Customize Portal Messages** click the link to the portal messages that you want to edit.
  - In other interfaces, make sure that **Customize Portal Messages** is selected, select the adjacent **Edit** icon, then select the message that you want to edit.
3. Edit the HTML message text, then select **Save**.
4. Select **OK**.



## Configuring disclaimer page for ethernet interface captive portals

While you can customize a disclaimer page for captive portals that connect via WiFi, the same can be done for wired connections. However, this can only be configured on the CLI Console, and only without configuring user groups.

When configuring a captive portal through the CLI, you may set `security-groups` to a specific user group. The result of this configuration will show an authentication form to users who wish to log in to the captive portal—**not** a disclaimer page. If you do not set any `security-groups` in your configuration, an "Allow all" status will be in effect, and the disclaimer page will be displayed for users.

The example CLI configuration below shows setting up a captive portal interface without setting security-groups, resulting in a disclaimer page for users:

```
config system interface
  edit "port1"
    set vdom "root"
    set ip 172.16.101.1 255.255.255.0
    set allowaccess ping https ssh snmp http
    set type physical
    set explicit-web-proxy enable
    set alias "LAN"
    set security-mode captive-portal
    set snmp-index 1
  next
end
```

## Roaming support

Client devices can maintain captive portal authentication as they roam across different APs. By maintaining a consistent authentication, uninterrupted access to latency sensitive applications such as VoIP is ensured.

The Cloud will push a random per-AP Network encryption key to the AP. The key is 32 bytes in length, and is used in captive portal fast roaming. All APs of an AP Network will use the same encryption key. This key is randomly generated, and will be updated daily.

## Session timeout interval for captive portal

The following syntax can be set to configure a session timeout interval in seconds for Captive Portal users. Set the range between 0 - 864000 (or no timeout to ten days). The default is set to 0.



This command is only available when **local-standalone** is set to **enable**, **security** is set to **captive-portal**, and then **portal-type** is set to either **cmcc** or **cmcc-macauth**.

### Syntax

```
config wireless-controller vap
  edit <name>
    ...
    set captive-portal-session-timeout-interval <seconds>
  next
end
```

## Configuration example - captive portal WiFi access control

In this scenario, you will configure the FortiGate for captive portal access so users can log on to your WiFi network.

You will create a user account (*rgreen*), add it to a user group (*employees*), create a captive portal SSID (*example-staff*), and configure a FortiAP unit. When the user attempts to browse the Internet, they will be redirected to the captive portal login page and asked to enter their username and password.

## 1. Enabling HTTPS authentication

Go to **User & Device > Authentication Settings**.

Under **Protocol Support**, enable **Redirect HTTP Challenge to a Secure Channel (HTTPS)**. This will make sure that user credentials are communicated securely through the captive portal.

## 2. Creating the user

Go to **User & Device > User Definition** and create a Local user (*rgreen*).

Create additional users if needed, and assign any authentication methods.

## 3. Creating the user group

Go to **User & Device > User Groups** and create a user group (*employees*).

Add **rgreen** to the group.

## 4. Creating the SSID

Go to **WiFi & Switch Controller > SSID** and configure the wireless network.

Some FortiGate models may show the GUI path as **WiFi & Switch Controller**.

Enter an **Interface Name** (*example-wifi*) and **IP/Network Mask**.

An address range under **DHCP Server** will be automatically configured.

Under **WiFi Settings**, enter an **SSID** name (*example-staff*), set **Security Mode** to **Captive Portal**, and add the **employees** user group.

## 5. Creating the security policy

Go to **Policy & Objects > Addresses** and create a new address for the SSID (*example-wifi-net*).

Set **Subnet/IP Range** to the same range set on the DHCP server in the previous step.

Set **Interface** to the SSID interface.

Go to **Policy & Objects > IPv4 Policy** and create a new policy for WiFi users to connect to the Internet.

Add both the **example-wifi-net** address and **employees** user group to **Source**.

## 6. Connecting and authorizing the FortiAP

Go to **Network > Interfaces** and edit an available interface.

Under **Address**, set **Addressing mode** to **Dedicated to Extension Device** and assign it an IP address.

Connect the FortiAP unit to the configured interface, then go to **WiFi & Switch Controller > Managed FortiAPs**.

The FortiAP is listed, but its **State** shows a greyed-out question mark — this is because it is waiting for authorization.

Highlight the FortiAP and select **Authorize**.

The question mark is now replaced by a red down-arrow — this is because it is authorized, but still offline.

Go to **WiFi & Switch Controller > FortiAP Profiles** and edit the profile.

For each radio, enable **Radio Resource Provision** and select your SSID.

Go back to **WiFi & Switch Controller > Managed FortiAPs** to verify that the FortiAP unit is online.

## 7. Results

When a user attempts to connect to the wireless network, they will be redirected to the captive portal login screen.

Members of the **employees** group must enter their **Username** and **Password**. The user will then be redirected to the URL originally requested.

On the FortiGate, go to **Monitor > WiFi Client Monitor** to verify that the user is authenticated.

# Configuring a WiFi LAN

When working with a FortiGate WiFi controller, you can configure your wireless network before you install any access points. If you are working with a standalone FortiWiFi unit, the access point hardware is already present but the configuration is quite similar. Both are covered in this section.

[Overview of WiFi controller configuration](#)

[Setting your geographic location](#)

[Creating a FortiAP profile](#)

[Defining a wireless network interface \(SSID\)](#)

[Defining SSID groups](#)

[Dynamic user VLAN assignment](#)

[Configuring user authentication](#)

[Configuring firewall policies for the SSID](#)

[Configuring the built-in access point on a FortiWiFi unit](#)

[Enforcing UTM policies on a local bridge SSID for managed smart APs](#)



On FortiGate model 30D, web-based manager configuration of the WiFi controller is disabled by default. To enable it, enter the following CLI commands:

```
config system global
    set gui-wireless-controller enable
end
```

The WiFi Controller and Switch Controller are enabled through the Feature Store (under **System > Feature Select**). However, they are separately enabled and configured to display in the GUI via the CLI.

To enable both WiFi and Switch controllers, enter the following:



```
config system global
    set wireless-controller enable
    set switch-controller enable
end
```

To enable the GUI display for both controllers, have also been separated:

```
config system settings
    set gui-wireless-controller enable
    set gui-switch-controller enable
end
```

If you want to connect and authorize external APs, such as FortiAP units, see the next chapter, [Access point deployment](#).

## Overview of WiFi controller configuration

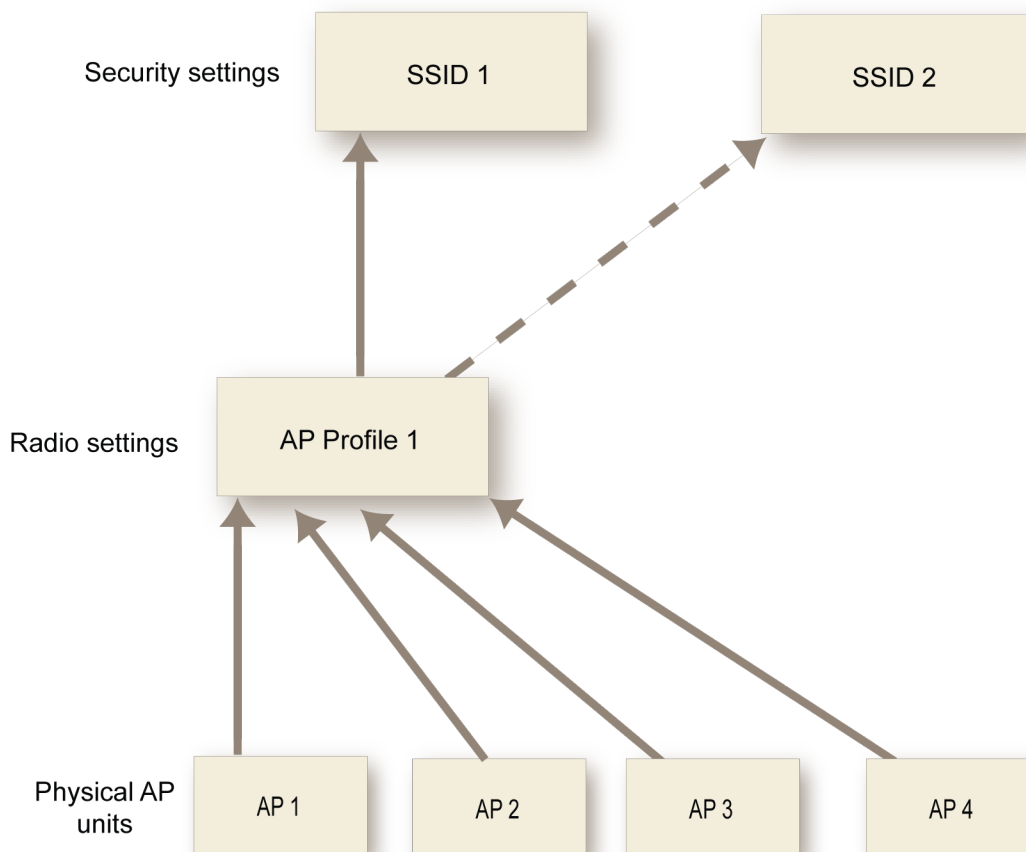
The FortiGate WiFi controller configuration is composed of three types of object, the SSID, the AP Profile and the physical Access Point.

- An **SSID** defines a virtual wireless network interface, including security settings. One SSID is sufficient for a wireless network, regardless how many physical access points are provided. You might, however, want to create multiple SSIDs to provide different services or privileges to different groups of users. Each SSID has separate firewall policies and authentication. Each radio in an access point can support up to 8 SSIDs.

A more common use of the term SSID is for the identifier that clients must use to connect to the wireless network. Each SSID (wireless interface) that you configure will have an SSID field for this identifier. In Managed Access Point configurations you choose wireless networks by SSID values. In firewall policies you choose wireless interfaces by their SSID name.

- An **AP Profile** defines the radio settings, such as band (802.11g for example) and channel selection. The AP Profile names the SSIDs to which it applies. Managed APs can use automatic profile settings or you can create AP profiles.
- **Managed Access Points** represent local wireless APs on FortiWiFi units and FortiAP units that the FortiGate unit has discovered. There is one managed access point definition for each AP device. An access point definition can use automatic AP profile settings or select a FortiAP Profile. When automatic profile settings are used, the managed AP definition also selects the SSIDs to be carried on the AP.

### Conceptual view of FortiGate WiFi controller configuration



### About SSIDs on FortiWiFi units

FortiWiFi units have a default SSID (wireless interface) named **wlan**. You can modify or delete this SSID as needed. As with external APs, the built-in wireless AP can be configured to carry any SSID.

The AP settings for the built-in wireless access point are located at **WiFi Controller > Local WiFi Radio**. The available operational settings are the same as those for external access points which are configured at **WiFi Controller > Managed FortiAPs**.

### Process to create a wireless network

To set up your wireless network, you will need to perform the following steps:

- Make sure the FortiGate wireless controller is configured for your geographic location. This ensures that the available radio channels and radio power are in compliance with the regulations in your region.
- Optionally, if you don't want to use automatic AP profile settings, configure a FortiAP profile, specifying the radio settings and the SSIDs to which they apply.
- Configure one or more SSIDs for your wireless network. The SSID configuration includes DHCP and DNS settings.
- Configure the user group and users for authentication on the WLAN.

- Configure the firewall policy for the WLAN.
- Optionally, customize the captive portal.
- Configure access points.  
Configuration of the built-in AP on FortiWiFi units is described in this chapter. Connection and configuration of FortiAP units is described in the next chapter, see [Access point deployment on page 54](#).

## Setting your geographic location

The maximum allowed transmitter power and permitted radio channels for WiFi networks depend on the region in which the network is located. By default, the WiFi controller is configured for the United States. If you are located in any other region, you need to set your location before you begin configuring wireless networks.

### To change the location setting - CLI

To change the country to France, for example, enter

```
config wireless-controller setting
  set country FR
end
```

To see the list of country codes, enter a question mark (“?”) instead of a country code.



Before changing the country setting, you must remove all FortiAP Profiles. To do this, go to **WiFi & Switch Controller > FortiAP Profiles**.

## View all country and regcodes/regulatory domains

The following CLI command can be entered to view a list of the country and regcodes/regulatory Domains supported by Fortinet:

```
cw_diag -c all-countries
```

Below is a table showing a sample of the list displayed by entering this command:

Country-code	Region-code	Domain	ISO-name	Name
0	A	FCC3 & FCCA	NA	NO_COUNTRY_SET
8	W	NULL1 & WORLD	AL	ALBANIA
12	W	NULL1 & WORLD	DZ	ALGERIA
16	A	FCC3 & FCCA	AS	AMERICAN SAMOA
...	...	...	...	...



## Creating a FortiAP profile

A FortiAP profile defines radio settings for a particular platform (FortiAP model). The profile also selects which SSIDs (virtual APs) the APs will carry. FortiAP units contain two radio transceivers, making it possible, for example, to provide both 2.4GHz 802.11b/g/n and 5GHz 802.11a/n service from the same access point. The radios can also be used for monitoring, used for the Rogue AP detection feature.

You can modify existing FortiAP profiles or create new ones of your own.



On FortiGate model 30D, web-based manager configuration of FortiAP Profiles is disabled by default. To enable AP profiles, enter the following CLI commands:

```
config system settings
  set gui-ap-profile enable
end
```

### To configure a FortiAP profile - web-based manager

1. Go to **WiFi & Switch Controller > FortiAP Profiles** and select **Create New**.
2. Enter a **Name** for the FortiAP Profile.
3. In **Platform**, select the FortiWiFi or FortiAP model to which this profile applies.
4. If split tunneling is used, in **Split Tunneling Subnets**, enter a comma-separated list all of the destination IP address ranges that should **not** be routed through the the FortiGate WiFi controller.
5. For each radio, enter:

<b>Mode</b>	Select the type of mode.  <b>Disable</b> – radio disabled <b>Access Point</b> – the platform is an access point <b>Dedicated Monitor</b> – the platform is a dedicated monitor. See <a href="#">Wireless network monitoring on page 114</a> .
<b>WIDS Profile</b>	Optionally, select a Wireless Intrusion Detection (WIDS) profile. See <a href="#">Protecting the WiFi network on page 108</a> .
<b>Radio Resource Provision</b>	Select to enable the radio resource provision feature. This feature measures utilization and interference on the available channels and selects the clearest channel at each access point. The measurement can be repeated periodically to respond to changing conditions.
<b>Client Load Balancing</b>	Select Frequency Handoff or AP Handoff as needed. See <a href="#">Access point deployment on page 54</a> .

<b>Band</b>	<p>Select the wireless protocols that you want to support. The available choices depend on the radio's capabilities. Where multiple protocols are supported, the letter suffixes are combined: "802.11g/b" means 802.11g and 802.11b.</p> <p>Note that on two-radio units such as the FortiAP-221C it is not possible to put both radios on the same band.</p>
<b>Channel Width</b>	Select channel width for 802.11ac or 802.11n on 5GHz.
<b>Short Guard Interval</b>	Select to enable the short guard interval for 802.11ac or 802.11n on 5GHz.
<b>Channels</b>	Select the channel or channels to include. The available channels depend on which IEEE wireless protocol you selected in <b>Band</b> . By default, all available channels are enabled.
<b>TX Power Control</b>	Enable automatic or manual adjustment of transmit power, specifying either minimum and maximum power levels in dBm or as a percentage.
<b>TX Power</b>	<p>When <b>TX Power Control</b> is set to <b>Auto</b>, the <b>TX Power</b> is set by default to a range of 10-17 dBm. Set the range between 1-20 for both the lower and upper limits.</p> <p>When <b>TX Power Control</b> is set to <b>Manual</b>, the <b>TX Power</b> is set by default to 100% of the maximum power permitted in your region. To change the level, drag the slider.</p>
<b>SSIDs</b>	<p>Select between <b>Auto</b> or <b>Manual</b>. Selecting <b>Auto</b> eliminates the need to re-edit the profile when new SSIDs are created. However, you can still select SSIDs individually using <b>Manual</b>.</p> <p>Note that automatic assignment of SSIDs (<b>Auto</b>) is not available for FortiAPs in <b>Local Bridge</b> mode. The option is hidden on both the Managed FortiAP settings and the FortiAP Profile assigned to that AP.</p>

Radio 1 settings are the same as Radio 2 settings except for the options for **Channel**.

Radio 2 settings are available only for FortiAP models with dual radios.

#### 6. Select **OK**.

### To configure a FortiAP profile - CLI

This example configures a FortiAP-220B to carry all SSIDs on Radio 1 but only SSID example\_wlan on Radio 2.

```
config wireless-controller wtp-profile
  edit guest_prof
    config platform
      set type 220B
    end
    config radio-1
      set mode ap
      set band 802.11g
      set vap-all enable
    end
```

```

config radio-2
    set mode ap
    set band 802.11g
    set vaps example_wlan
end
end

```

## Defining a wireless network interface (SSID)

You begin configuring your wireless network by defining one or more SSIDs to which your users will connect. When you create an SSID, a virtual network interface is also created with the **Name** you specified in the SSID configuration. You can configure the settings of an existing SSID in either **WiFi & Switch Controller > SSID** or **System > Network > Interfaces**.



If a software switch interface contains an SSID (but only one), the WiFi SSID settings are available in the switch interface settings.

### To create a new SSID

1. Go to **WiFi & Switch Controller > SSID** and select **Create New > SSID**.
2. Fill in the SSID fields as described below.

### To configure the settings of an existing SSID

1. Either
  - Go to **WiFi & Switch Controller > SSID**.
 or
  - Go to **Network > Interfaces**.  
WiFi interfaces list the SSID beside the interface **Name**.
2. Edit a WiFi interface, modifying the SSID fields as needed.

### SSID fields

<b>Interface Name</b>	Enter a name for the SSID interface.
<b>Type</b>	WiFi SSID.
<b>Traffic Mode</b>	<p><b>Tunnel to Wireless Controller</b> — Data for WLAN passes through WiFi Controller. This is the default.</p> <p><b>Local bridge with FortiAP's Interface</b> — FortiAP unit Ethernet and WiFi interfaces are bridged.</p> <p><b>Mesh Downlink</b> — Radio receives data for WLAN from mesh backhaul SSID.</p>

<b>IP/Network Mask</b>	Enter the IP address and netmask for the SSID.
<b>IPv6 Address</b>	Enter the IPv6 address. This is available only when IPv6 has been enabled on the unit.
<b>Administrative Access</b>	Select which types of administrative access are permitted on this SSID.
<b>IPv6 Administrative Access</b>	If you have IPv6 addresses, select the permitted IPv6 administrative access types for this SSID.
<b>DHCP Server</b>	<p>To assign IP addresses to clients, enable DHCP server. You can define IP address ranges for a DHCP server on the FortiGate unit or relay DHCP requests to an external server.</p> <p>If the unit is in transparent mode, the DHCP server settings will be unavailable.</p> <p>For more information, see <a href="#">Configuring DHCP for WiFi clients on page 38</a>.</p>
<b>Device Detection</b>	Detect connected device type. Enabled by default.
<b>Active Scanning</b>	Enabled by default.
<b>WiFi Settings</b>	
<b>SSID</b>	Enter the SSID. By default, this field contains <code>fortinet</code> .
<b>Security Mode</b>	Select the security mode for the wireless interface. Wireless users must use the same security mode to be able to connect to this wireless interface. Additional security mode options are available in the CLI. For more information, see <a href="#">Configuring security on page 39</a> .
	<b>Captive Portal</b> – authenticates users through a customizable web page.
	<b>WPA2-Personal</b> – WPA2 is WiFi Protected Access version 2. There is one pre-shared key (password) that all users use.
	<b>WPA2-Personal with Captive Portal</b> – The user will need to know the pre-shared key and will also be authenticated through the custom portal.
	<b>WPA2-Enterprise</b> – similar to WPA2-Personal, but is best used for enterprise networks. Each user is separately authenticated by user name and password.
<b>Pre-shared Key</b>	Available only when <b>Security Mode</b> is <b>WPA2-Personal</b> . Enter the encryption key that the clients must use.

<b>Authentication</b>	Available only when <b>Security Mode</b> is <b>WPA2-Enterprise</b> .  Select one of the following:  <b>RADIUS Server</b> — Select the RADIUS server that will authenticate the clients. <b>Local</b> – Select the user group(s) that can authenticate.
<b>Portal Type</b>	Available only when <b>Security Mode</b> is <b>Captive Portal</b> . Choose the captive portal type. Authentication is available with or without a usage policy disclaimer notice.
<b>Authentication Portal</b>	<b>Local</b> - portal hosted on the FortiGate unit <b>External</b> - enter FQDN or IP address of external portal
<b>User Groups</b>	Select permitted user groups for captive portal authentication.
<b>Exempt List</b>	Select exempt lists whose members will not be subject to captive portal authentication.
<b>Customize Portal Messages</b>	Click the listed portal pages to edit them.
<b>Redirect after Captive Portal</b>	Optionally, select <b>Specific URL</b> and enter a URL for user redirection after captive portal authentication. By default, users are redirected to the URL that they originally requested.
<b>Allow New WiFi Client Connections When Controller Is Down</b>	This option is available for local bridge SSIDs with WPA-Personal security. See <a href="#">Combining WiFi and wired networks with a software switch on page 88</a> .
<b>Broadcast SSID</b>	Optionally, disable broadcast of SSID. By default, the SSID is broadcast. For more information, see <a href="#">Introduction to wireless networking on page 12</a> .
<b>Schedule</b>	Select when the SSID is enabled. You can choose any schedule defined in <b>Policy &amp; Objects &gt; Objects &gt; Schedules</b> .
<b>Block Intra-SSID Traffic</b>	Select to enable the unit to block intra-SSID traffic.
<b>Maximum Clients</b>	Select to limit the number of clients permitted to connect simultaneously. Enter the limit value.
<b>Split Tunneling</b>	Select to enable some subnets to remain local to the remote FortiAP. Traffic for these networks is not routed through the WiFi Controller. Specify split-tunnel networks in the FortiAP Profile. See <a href="#">Split tunneling on page 95</a> .
<b>Optional VLAN ID</b>	Enter the ID of the VLAN this SSID belongs to. Enter 0 for non-VLAN operation.

<b>Enable Explicit Web Proxy</b>	Select to enable explicit web proxy for the SSID.
<b>Listen for RADIUS Accounting Messages</b>	Enable if you are using RADIUS-based single sign-on (SSO).
<b>Secondary IP Address</b>	Optionally, enable and define secondary IP addresses. Administrative access can be enabled on secondary interfaces.
<b>Comments</b>	Enter a description or comment for the SSID.

### To configure a virtual access point (SSID) - CLI

The example below creates an access point with SSID “example” and WPA2-Personal security. The wireless interface is named example\_wlan.

WiFi SSIDs include a schedule that determines when the WiFi network is available. The default schedule is Always. You can choose any schedule (but not schedule group) that is defined in **Policy & Objects > Objects > Schedules**.

```
config wireless-controller vap
  edit example_wlan
    set ssid "example"
    set broadcast-ssid enable
    set security wpa2-only-personal
    set passphrase "hardtoguess"
    set schedule always
    set vdom root
  end
config system interface
  edit example_wlan
    set ip 10.10.120.1 255.255.255.0
  end
```

## Configuring DHCP for WiFi clients

Wireless clients need to have IP addresses. If you use RADIUS authentication, each user’s IP address can be stored in the Framed-IP-Address attribute. Otherwise, you need to configure a DHCP server on the WLAN interface to assign IP addresses to wireless clients.

### To configure a DHCP server for WiFi clients - web-based manager

1. Go to **WiFi & Switch Controller > SSID** and edit your SSID entry.
2. In **DHCP Server** select **Enable**.
3. In **Address Range**, select **Create New**.
4. In the **Starting IP** and **End IP** fields, enter the IP address range to assign.  
By default an address range is created in the same subnet as the wireless interface IP address, but not including that address.
5. Set the **Netmask** to an appropriate value, such as 255.255.255.0.
6. Set the **Default Gateway to Same as Interface IP**.

7. Set the **DNS Server** to **Same as System DNS**.
8. If you want to restrict access to the wireless network by MAC address, see [Adding a MAC filter on page 41](#).
9. Select **OK**.

### To configure a DHCP server for WiFi clients - CLI

In this example, WiFi clients on the `example_wlan` interface are assigned addresses in the 10.10.120.2-9 range to connect with the WiFi access point on 10.10.120.1.

```
config system dhcp server
edit 0
set default-gateway 10.10.120.1
set dns-service default
set interface example_wlan
set netmask 255.255.255.0
config ip-range
edit 1
set end-ip 10.10.120.9
set start-ip 10.10.120.2
end
end
```



You cannot delete an SSID (wireless interface) that has DHCP enabled on it.

## Configuring security

Using the web-based manager, you can configure captive portal security or WiFi Protected Access version 2 (WPA2) security modes WPA2-Personal and WPA2-Enterprise. Using the CLI, you can also choose WPA/WPA2 modes that support both WPA version 1 and WPA version 2.

WPA2 security with a pre-shared key for authentication is called WPA2-Personal. This can work well for one person or a small group of trusted people. But, as the number of users increases, it is difficult to distribute new keys securely and there is increased risk that the key could fall into the wrong hands.

A more secure form of WPA2 security is WPA2-Enterprise. Users each have their own authentication credentials, verified through an authentication server, usually RADIUS. FortiOS can also authenticate WPA2-Enterprise users through its built-in user group functionality. FortiGate user groups can include RADIUS servers and can select users by RADIUS user group. This makes possible Role-Based Access Control (RBAC).

By default, WPA2 security encrypts communication using Advanced Encryption Standard (AES). But some older wireless clients support only Temporal Key Integrity Protocol (TKIP). You can change the encryption to TKIP or negotiable TKIP-AES in the CLI. For example, to accommodate clients with either TKIP or AES, enter:

```
config wireless-controller vap
edit example_wlan
set security wpa-personal
set passphrase "hardtoguess"
set encrypt TKIP-AES
end
```

Captive portal security connects users to an open web portal defined in replacement messages. To navigate to any location beyond the web portal, the user must pass FortiGate user authentication.

## WPA-Personal security

WPA2-Personal security setup requires only the preshared key that you will provide to your clients.

### To configure WPA2-Personal security - web-based manager

1. Go to **WiFi & Switch Controller > SSID** and edit your SSID entry.
2. In **Security Mode**, select **WPA2 Personal**.
3. In **Pre-shared Key**, enter a key between 8 and 63 characters long.
4. Select **OK**.

### To configure WPA2-Personal security - CLI

```
config wireless-controller vap
  edit example_wlan
    set security wpa2-personal
    set passphrase "hardtoguess"
  end
```

## WPA-Enterprise security

If you will use FortiOS user groups for authentication, go to **User & Device > User > User Groups** and create those groups first. The groups should be Firewall groups.

If you will use a RADIUS server to authenticate wireless clients, you must first configure the FortiGate unit to access the RADIUS server.

### To configure FortiGate unit access to the RADIUS server - web-based manager

1. Go to **User & Device > RADIUS Servers** and select **Create New**.
2. Enter a **Name** for the server.
3. In **Primary Server Name/IP**, enter the network name or IP address for the server.
4. In **Primary Server Secret**, enter the shared secret used to access the server.
5. Optionally, enter the information for a secondary or backup RADIUS server.
6. Select **OK**.

### To configure the FortiGate unit to access the RADIUS server - CLI

```
config user radius
  edit exampleRADIUS
    set auth-type auto
    set server 10.11.102.100
    set secret aoewmntiasf
  end
```

## RADIUS Change of Authorization (CoA) support

The CoA feature enables the FortiGate to receive a client disconnect message from the RADIUS server. This is used to disconnect clients when their time, credit or bandwidth had been used up. Enable this on the RADIUS server using the CLI:

```
config user radius
  edit <name>
    set radius-coa enable
```



```
end
```

### To configure WPA-Enterprise security - web-based manager

1. Go to **WiFi & Switch Controller > SSID** and edit your SSID entry.
2. In **Security Mode**, select **WPA2 Enterprise**.
3. In **Authentication**, do one of the following:
  - If you will use a RADIUS server for authentication, select **RADIUS** Server and then select the RADIUS server.
  - If you will use a local user group for authentication, select **Local** and then select the user group(s) permitted to use the wireless network.
4. Select **OK**.

### To configure WPA-Enterprise security - CLI

```
config wireless-controller vap
edit example_wlan
    set security wpa2-enterprise
    set auth radius
    set radius-server exampleRADIUS
end
```

## Captive portal security

Captive portal security provides an access point that initially appears open. The wireless client can connect to the AP with no security credentials. The AP responds to the client's first HTTP request with a web page requesting user name and password. Until the user enters valid credentials, no communication beyond the AP is permitted.

The captive portal can be hosted on the FortiGate unit, or externally. For details see

[Configuring WiFi captive portal security - FortiGate captive portal on page 43](#)

[Configuring WiFi captive portal security - external server on page 43](#)

For general information about captive portals, see the Captive Portal chapter of the Authentication Guide.

## Adding a MAC filter

On each SSID, you can create a MAC address filter list to either permit or exclude a list of clients identified by their MAC addresses.

This is actually not as secure as it appears. Someone seeking unauthorized access to your network can obtain MAC addresses from wireless traffic and use them to impersonate legitimate users. A MAC filter list should only be used in conjunction with other security measures such as encryption.

### To configure a MAC filter - web-based manager

1. Go to **WiFi & Switch Controller > SSID** and edit your SSID entry.
2. In the **DHCP Server** section, expand **Advanced**.
3. In **MAC Reservation + Access Control**, double-click in the **Unknown MAC Addresses** line and select **Assign IP** or **Block**, as needed.  
By default, unlisted MAC addresses are assigned an IP address automatically.
4. In **MAC Reservation + Access Control**, select **Create New**.

5. Enter a MAC address in the **MAC** field.
6. In **IP or Action**, select one of:
  - **Reserve IP** — enter the IP address that is always assigned to this MAC address.
  - **Assign IP** — an IP address is assigned to this MAC address automatically.
  - **Block** — This MAC address will not be assigned an IP address.
7. Repeat steps 4 through 6 for each additional MAC address that you want to add.
8. Select **OK**.

### To configure a MAC filter - CLI

1. Enter
 

```
config system dhcp server
show
```
2. Find the entry where `interface` is your WiFi interface. Edit that entry and configure the MAC filter. In this example, the MAC address 11:11:11:11:11:11 will be excluded. Unlisted MAC addresses will be assigned an IP address automatically.
 

```
edit 3
config reserved-address
edit 1
set action block
set mac 11:11:11:11:11:11
end
set mac-acl-default-action assign
end
```

## Limiting the number of clients

You might want to prevent overloading of your access point by limiting the number of clients who can associate with it at the same time. Limits can be applied per SSID, per AP, or per radio.

### To limit the number of clients per SSID - GUI

1. Go to **WiFi & Switch Controller > SSID** and edit your SSID.
2. Turn on **Maximum Clients** and enter the maximum number of clients in **Limit Concurrent WiFi Clients**.

### To limit the number of clients per AP- CLI

Edit the wtp-profile (FortiAP profile), like this:

```
config wireless-controller wtp-profile
edit "FAP221C-default"
set max-clients 30
end
```

### To limit the number of clients per radio - CLI

Edit the wtp-profile (FortiAP profile), like this:

```
config wireless-controller wtp-profile
edit "FAP221C-default"
config radio-1
set max-clients 10
```

```

end
config radio-2
    set max-clients 30
end
end

```

## Multicast enhancement

FortiOS can translate multicast traffic into unicast traffic to send to clients, maintaining its own multicast client through IGMP snooping. You can configure this in the CLI:

```

config wireless-controller vap
    edit example_wlan
        set multicast-enhance enable
        set me-disable-thresh 32
    end
end

```

If the number of clients on the SSID is larger than `me-disable-thresh`, multicast enhancement is disabled.

## Configuring WiFi captive portal security - FortiGate captive portal

The built-in FortiGate captive portal is simpler than an external portal. It can even be customized if needed.

**To configure a WiFi Captive Portal - web-based manager:**

1. Go to **WiFi & Switch Controller > SSID** and create your SSID.  
If the SSID already exists, you can edit the SSID or you can edit the WiFi interface in **Network > Interfaces**.
2. In **Security Mode**, select **Captive Portal**.
3. Enter

<b>Portal Type</b>	The portal can provide authentication and/or disclaimer, or perform user email address collection. See <a href="#">Defining a wireless network interface (SSID) on page 35</a> .
<b>Authentication Portal</b>	Local
<b>User Groups</b>	Select permitted user groups or select <b>Use Groups from Policies</b> , which permits the groups specified in the security policy.
<b>Exempt List</b>	Select exempt lists whose members will not be subject to captive portal authentication.
<b>Customize Portal Messages</b>	Click the link of the portal page that you want to modify. For more information see the Captive Portal chapter of the Authentication Guide.

4. Select **OK**.

## Configuring WiFi captive portal security - external server

An external captive portal is a web page on a web server. The essential part of the web portal page is a script that gathers the user's logon credentials and sends back to the FortiGate a specifically-formatted POST message. The portal page can also contain links to local information such as legal notices, terms of service and so on.

Without authenticating, the user cannot access any other information. This is sometimes called a “walled garden”.

On the captive portal page, the user submits credentials, which the script returns to the FortiGate at the URL **https://<FGT\_IP>:1000/fgtauth** with data

**magic=session\_id&username=<username>&password=<password>**.

(The magic value was provided in the initial FortiGate request to the web server.)

To ensure that credentials are communicated securely, enable the use of HTTPS for authentication:

```
config user setting
    set auth-secure-http enable
end
```

### To configure use of an external WiFi Captive Portal - web-based manager:

1. Go to **WiFi & Switch Controller > SSID** and create your SSID.  
If the SSID already exists, you can edit the SSID or you can edit the WiFi interface in **Network > Interfaces**.
2. In **Security Mode**, select **Captive Portal**.
3. Enter

<b>Portal Type</b>	The portal can provide authentication and/or disclaimer, or perform user email address collection.
<b>Authentication Portal</b>	External - enter the FQDN or IP address of the external portal. Typically, this is the URL of a script. Do <b>not</b> include the protocol (http:// or https://) part of the URL.
<b>User Groups</b>	Select permitted user groups or select <b>Use Groups from Policies</b> , which permits the groups specified in the security policy.
<b>Exempt List</b>	Select exempt lists whose members will not be subject to captive portal authentication.
<b>Redirect after Captive Portal</b>	Original Request  Specific URL - enter URL

4. Select **OK**.

## Defining SSID groups

Optionally, you can define SSID groups. An SSID group has SSIDs as members and can be specified just like an SSID in a FortiAP Profile.

### To create an SSID group - GUI

Go to **WiFi & Switch Controller > SSID** and select **Create New > SSID Group**. Give the group a **Name** and choose **Members** (SSIDs, but not SSID groups).

**To create an SSID group - CLI:**

```
config wireless-controller vap-group
edit vap-group-name
set vaps "ssid1" "ssid2"
end
```

## Dynamic user VLAN assignment

Clients connecting to the WiFi network can be assigned to a VLAN. You can do this with RADIUS attributes when the user authenticates or with VLAN pooling when the client associates with a particular FortiAP. You cannot use both of these methods at the same time.

### VLAN assignment by RADIUS

You can assign each individual user to a VLAN based on information stored in the RADIUS authentication server. If the user's RADIUS record does not specify a VLAN ID, the user is assigned to the default VLAN for the SSID.

The RADIUS user attributes used for the VLAN ID assignment are:

IETF 64 (Tunnel Type)—Set this to VLAN.

IETF 65 (Tunnel Medium Type)—Set this to 802

IETF 81 (Tunnel Private Group ID)—Set this to the VLAN ID.

To configure dynamic VLAN assignment, you need to:

1. Configure access to the RADIUS server.
2. Create the SSID and enable dynamic VLAN assignment.
3. Create a FortiAP Profile and add the local bridge mode SSID to it.
4. Create the VLAN interfaces and their DHCP servers.
5. Create security policies to allow communication from the VLAN interfaces to the Internet.
6. Authorize the FortiAP unit and assign the FortiAP Profile to it.

**To configure access to the RADIUS server**

1. Go to **User & Device > RADIUS Servers** and select **Create New**.
2. Enter a **Name**, the name or IP address in **Primary Server IP/Name**, and the server secret in **Primary Server Secret**.
3. Select **OK**.

**To create the dynamic VLAN SSID**

1. Go to **WiFi & Switch Controller > SSID**, select **Create New > SSID** and enter:

<b>Name</b>	An identifier, such as dynamic_vlan_ssid.
<b>Traffic Mode</b>	Local bridge or Tunnel, as needed.

<b>SSID</b>	An identifier, such as DYNSSID.
<b>Security Mode</b>	WPA2 Enterprise
<b>Authentication</b>	RADIUS Server. Select the RADIUS server that you configured.

2. Select **OK**.
3. Enable dynamic VLAN in the CLI. Optionally, you can also assign a VLAN ID to set the default VLAN for users without a VLAN assignment.

```
config wireless-controller vap
  edit dynamic_vlan_ssid
    set dynamic-vlan enable
    set vlanid 10
  end
```

### To create the FortiAP profile for the dynamic VLAN SSID

1. Go to **WiFi & Switch Controller > FortiAP Profiles**, select **Create New** and enter:

<b>Name</b>	A name for the profile, such as dyn_vlan_profile.
<b>Platform</b>	The FortiAP model you are using. If you use more than one model of FortiAP, you will need a FortiAP Profile for each model.
<b>Radio 1 and Radio 2</b>	
<b>SSID</b>	Select the SSID you created (example dynamic_vlan_ssid). Do not add other SSIDs.

2. Adjust other radio settings as needed.
3. Select **OK**.

### To create the VLAN interfaces

1. Go to **Network > Interfaces** and select **Create New > Interface**.
2. Enter:

<b>Name</b>	A name for the VLAN interface, such as VLAN100.
<b>Interface</b>	The physical interface associated with the VLAN interface.
<b>VLAN ID</b>	The numeric VLAN ID, for example 100.
<b>Addressing mode</b>	Select <b>Manual</b> and enter the IP address / Network Mask for the virtual interface.
<b>DHCP Server</b>	Enable and then select <b>Create New</b> to create an address range.

3. Select **OK**.
4. Repeat the preceding steps to create other VLANs as needed.

Security policies determine which VLANs can communicate with which other interfaces. These are the simple Firewall Address policy without authentication. Users are assigned to the appropriate VLAN when they authenticate.

#### To connect and authorize the FortiAP unit

1. Connect the FortiAP unit to the FortiGate unit.
2. Go to **WiFi & Switch Controller > Managed FortiAPs**.
3. When the FortiAP unit is listed, double-click the entry to edit it.
4. In **FortiAP Profile**, select the FortiAP Profile that you created.
5. Select **Authorize**.
6. Select **OK**.

## VLAN assignment by VLAN pool

In an SSID, you can define a VLAN pool. As clients associate to an AP, they are assigned to a VLAN. A VLAN pool can

- assign a specific VLAN based on the AP's FortiAP group, usually for network configuration reasons, or
- assign one of several available VLANs for network load balancing purposes (tunnel mode SSIDs only)

#### To assign a VLAN by FortiAP group - CLI

In this example, VLAN 101, 102, or 103 is assigned depending on the AP's FortiAP group.

```
config wireless-controller vap
  edit wlan
    set vlan-pooling wtp-group
    config vlan-pool
      edit 101
        set wtp-group wtpgrp1
      next
      edit 102
        set wtp-group wtpgrp2
      next
      edit 103
        set wtp-group wtpgrp3
      end
    end
  end
end
```

## Load balancing

There are two VLAN pooling methods used for load balancing:

The choice of VLAN can be based on any one of the following criteria:

- **round-robin** - from the VLAN pool, choose the VLAN with the smallest number of clients
- **hash** - choose a VLAN from the VLAN pool based on a hash of the current number of SSID clients and the number of entries in the VLAN pool

If the VLAN pool contains no valid VLAN ID, the SSID's static VLAN ID setting is used.

### To assign a VLAN by round-robin selection - CLI

In this example, VLAN 101, 102, or 103 is assigned using the round-robin method:

```
config wireless-controller vap
  edit wlan
    set vlan-pooling round-robin
    config vlan-pool
      edit 101
      next
      edit 102
      next
      edit 103
      end
    end
  end
end
```

### To assign a VLAN by hash-based selection - CLI

In this example, VLAN 101, 102, or 103 is assigned using the hash method:

```
config wireless-controller vap
  edit wlan
    set vlan-pooling hash
    config vlan-pool
      edit 101
      next
      edit 102
      next
      edit 103
      end
    end
  end
end
```

## Configuring user authentication

You can perform user authentication when the wireless client joins the wireless network and when the wireless user communicates with another network through a firewall policy. WEP and WPA-Personal security rely on legitimate users knowing the correct key or passphrase for the wireless network. The more users you have, the more likely it is that the key or passphrase will become known to unauthorized people. WPA-Enterprise and captive portal security provide separate credentials for each user. User accounts can be managed through FortiGate user groups or an external RADIUS authentication server.

### WPA2 Enterprise authentication

Enterprise authentication can be based on the local FortiGate user database or on a remote RADIUS server. Local authentication is essentially the same for WiFi users as it is for wired users, except that authentication for WiFi users occurs when they associate their device with the AP. Therefore, enterprise authentication must be configured in the SSID. WiFi users can belong to user groups just the same as wired users and security policies will determine which network services they can access.

If your WiFi network uses WPA2 Enterprise authentication verified by a RADIUS server, you need to configure the FortiGate unit to connect to that RADIUS server.



### Configuring connection to a RADIUS server - web-based manager

1. Go to **User & Device > RADIUS Servers** and select **Create New**.
2. Enter a **Name** for the server.  
This name is used in FortiGate configurations. It is not the actual name of the server.
3. In **Primary Server Name/IP**, enter the network name or IP address for the server.
4. In **Primary Server Secret**, enter the shared secret used to access the server.
5. Optionally, enter the information for a secondary or backup RADIUS server.
6. Select **OK**.

### To configure the FortiGate unit to access the RADIUS server - CLI

```
config user radius
  edit exampleRADIUS
    set auth-type auto
    set server 10.11.102.100
    set secret aoewmntiasf
  end
```

To implement WPA2 Enterprise security, you select this server in the SSID security settings. See [Configuring user authentication on page 48](#).

To use the RADIUS server for authentication, you can create individual FortiGate user accounts that specify the authentication server instead of a password, and you then add those accounts to a user group. Or, you can add the authentication server to a FortiGate user group, making all accounts on that server members of the user group.

### Creating a wireless user group

Most wireless networks require authenticated access. To enable creation of firewall policies specific to WiFi users, you should create at least one WiFi user group. You can add or remove users later. There are two types of user group to consider:

- A Firewall user group can contain user accounts stored on the FortiGate unit or external authentication servers such as RADIUS that contain and verify user credentials.
- A Fortinet single sign-on (FSSO) user group is used for integration with Windows Active Directory or Novell eDirectory. The group can contain Windows or Novell user groups who will be permitted access to the wireless LAN.

## WiFi single sign-on (WSSO) authentication

WSSO is RADIUS-based authentication that passes the user's user group memberships to the FortiGate. For each user, the RADIUS server must provide user group information in the Fortinet-Group-Name attribute. This information is stored in the server's database. After the user authenticates, security policies provide access to network services based on user groups.

1. Configure the RADIUS server to return the Fortinet-Group-Name attribute for each user.
2. Configure the FortiGate to access the RADIUS server, as described in [WPA2 Enterprise authentication on page 48](#).
3. Create firewall user groups on the FortiGate with the same names as the user groups listed in the RADIUS database. Leave the groups empty.
4. In the SSID choose WPA2-Enterprise authentication. In the **Authentication** field, select **RADIUS Server** and choose the RADIUS server that you configured.
5. Create security policies as needed, using user groups (**Source User(s)** field) to control access.

When a user authenticates by WSSO, the firewall monitor **Monitor > Firewall User Monitor**) shows the authentication method as WSSO.

## Assigning WiFi users to VLANs dynamically

Some enterprise networks use Virtual LANs (VLANs) to separate traffic. In this environment, to extend network access to WiFi users might appear to require multiple SSIDs. But it is possible to automatically assign each user to their appropriate VLAN from a single SSID. To accomplish this requires RADIUS authentication that passes the appropriate VLAN ID to the FortiGate by RADIUS attributes. Each user's VLAN assignment is stored in the user database of the RADIUS server.

1. Configure the RADIUS server to return the following attributes for each user:  
Tunnel-Type (value: VLAN)  
Tunnel-Medium-Type (value: IEEE-802)  
Tunnel\_Private-Group-Id (value: the VLAN ID for the user's VLAN)
2. Configure the FortiGate to access the RADIUS server.
3. Configure the SSID with WPA2-Enterprise authentication. In the **Authentication** field, select **RADIUS Server** and choose the RADIUS server that you will use.
4. Create VLAN subinterfaces on the SSID interface, one for each VLAN. Set the VLAN ID of each as appropriate. You can do this on the **Network > Interfaces** page.
5. Enable Dynamic VLAN assignment for the SSID. For example, if the SSID interface is "office", enter:

```
config wireless-controller vap
  edit office
    set dynamic-vlan enable
  end
```
6. Create security policies for each VLAN. These policies have a WiFi VLAN subinterface as **Incoming Interface** and allow traffic to flow to whichever **Outgoing Interface** these VLAN users will be allowed to access.

## MAC-based authentication

Wireless clients can also be supplementally authenticated by MAC address. A RADIUS server stores the allowed MAC address for each client and the wireless controller checks the MAC address independently of other authentication methods.

MAC-based authentication must be configured in the CLI. In the following example, MAC-based authentication is added to an existing access point "vap1" to use RADIUS server hq\_radius (configured on the FortiGate):

```
config wireless-controller vap
  edit vap1
    set radius-mac-auth enable
    set radius-mac-auth-server hq_radius
  end
```

## Authenticating guest WiFi users

The FortiOS Guest Management feature enables you to easily add guest accounts to your FortiGate unit. These accounts are authenticate guest WiFi users for temporary access to a WiFi network managed by a FortiGate unit. To implement guest access, you need to

1. Go to **User & Device > User Groups** and create one or more guest user groups.
2. Go to **User & Device > Guest Management** to create guest accounts. You can print the guest account credentials or send them to the user as an email or SMS message.
3. Go to **WiFi & Switch Controller > SSID** and configure your WiFi SSID to use captive portal authentication. Select the guest user group(s) that you created.

Guest users can log into the WiFi captive portal with their guest account credentials until the account expires. For more detailed information about creating guest accounts, see "Managing Guest Access" in the Authentication chapter of the FortiOS Handbook.

## Configuring firewall policies for the SSID

For users on the WiFi LAN to communicate with other networks, firewall policies are required. This section describes creating a WiFi network to Internet policy.

Before you create firewall policies, you need to define any firewall addresses you will need.

### To create a firewall address for WiFi users - web-based manager

1. Go to **Policy & Objects > Addresses**.
2. Select **Create New**, enter the following information and select **OK**.

<b>Name</b>	Enter a name for the address, wifi_net for example.
<b>Type</b>	Select <b>Subnet</b> .
<b>Subnet / IP Range</b>	Enter the subnet address, 10.10.110.0/24 for example.
<b>Interface</b>	Select the interface where this address is used, e.g., example_wifi

### To create a firewall address for WiFi users - CLI

```
config firewall address
edit "wifi_net"
set associated-interface "example_wifi"
set subnet 10.10.110.0 255.255.255.0
end
```

### To create a firewall policy - web-based manager

1. Go to **Policy & Objects > IPv4 Policy** and select **Create New**.
2. In **Incoming Interface**, select the wireless interface.
3. In **Source Address**, select the address of your WiFi network, wifi\_net for example.
4. In **Outgoing Interface**, select the Internet interface, for example, port1.
5. In **Destination Address**, select **All**.
6. In **Service**, select **ALL**, or select the particular services that you want to allow, and then select the right arrow button to move the service to the **Selected Services** list.
7. In **Schedule**, select **always**, unless you want to define a schedule for limited hours.
8. In **Action**, select **ACCEPT**.
9. Select **Enable NAT**.

10. Optionally, set up UTM features for wireless users.
11. Select **OK**.

### To create a firewall policy - CLI

```
config firewall policy
  edit 0
    set srcintf "example_wifi"
    set dstintf "port1"
    set srcaddr "wifi_net"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ANY"
    set nat enable
  end
```

## Configuring the built-in access point on a FortiWiFi unit

Both FortiGate and FortiWiFi units have the WiFi controller feature. If you configure a WiFi network on a FortiWiFi unit, you can also use the built-in wireless capabilities in your WiFi network as one of the access points.

If Virtual Domains are enabled, you must select the VDOM to which the built-in access point belongs. You do this in the CLI. For example:

```
config wireless-controller global
  set local-radio-vdom vdom1
end
```

### To configure the FortiWiFi unit's built-in WiFi access point

1. Go to **WiFi Controller > Local WiFi Radio**.
2. Make sure that **Enable WiFi Radio** is selected.
3. In **SSID**, if you do not want this AP to carry all SSIDs, select **Select SSIDs** and then select the required SSIDs.
4. Optionally, adjust the **TX Power** slider.  
If you have selected your location correctly (see [Configuring the built-in access point on a FortiWiFi unit on page 52](#)), the 100% setting corresponds to the maximum power allowed in your region.
5. If you do not want the built-in WiFi radio to be used for rogue scanning, select **Do not participate in Rogue AP scanning**.
6. Select **OK**.

If you want to connect external APs, such as FortiAP units, see the next chapter, [Access point deployment](#).

## Enforcing UTM policies on a local bridge SSID for managed smart APs

The `config wireless-controller utm-profile` command lets administrators configure UTM profiles in order to enforce UTM policies on a local bridge SSID when Smart AP's are managed by FortiGate.

As a result, these UTM profiles can also be assigned under `config wireless-controller vap`.

Please note that this is only supported in Bridge-mode.

In addition, a new diagnose command has been introduced to determine the status of the `cw_acd` daemon, which handles the communication between FortiGate and APs.

Note that the default `utm-profile` available (named `wifi-default`) has all applicable options within the command set to `wifi-default`.

Use "?" to view all available profiles to assign, for example, "set ips-sensor ?".

**Syntax:**

```
config wireless-controller utm-profile
  edit <name>
    set comment <comment>
    set utm-log {enable | disable}
    set ips-sensor <name>
    set application-list <name>
    set antivirus-profile <name>
    set webfilter-profile <name>
    set firewall-policy <id>
    set scan-botnet-connections {disable | block | monitor}
  next
end

config wireless-controller vap
  edit <name>
    set utm-profile <name>
  next
end
```

To debug the `cw_acd_helper` daemon, use the following diagnose command:

```
diagnose wireless-controller wlac_hlp
```

# Access point deployment

This chapter describes how to configure access points for your wireless network.

[Overview](#)

[Network topology for managed APs](#)

[Discovering and authorizing APs](#)

[Advanced WiFi controller discovery](#)

[Wireless client load balancing for high-density deployments](#)

[FortiAP groups](#)

[LAN port options](#)

[Preventing IP fragmentation of packets in CAPWAP tunnels](#)

[LED options](#)

[CAPWAP bandwidth formula](#)

## Overview

FortiAP units discover WiFi controllers. The administrator of the WiFi controller authorizes the FortiAP units that the controller will manage.

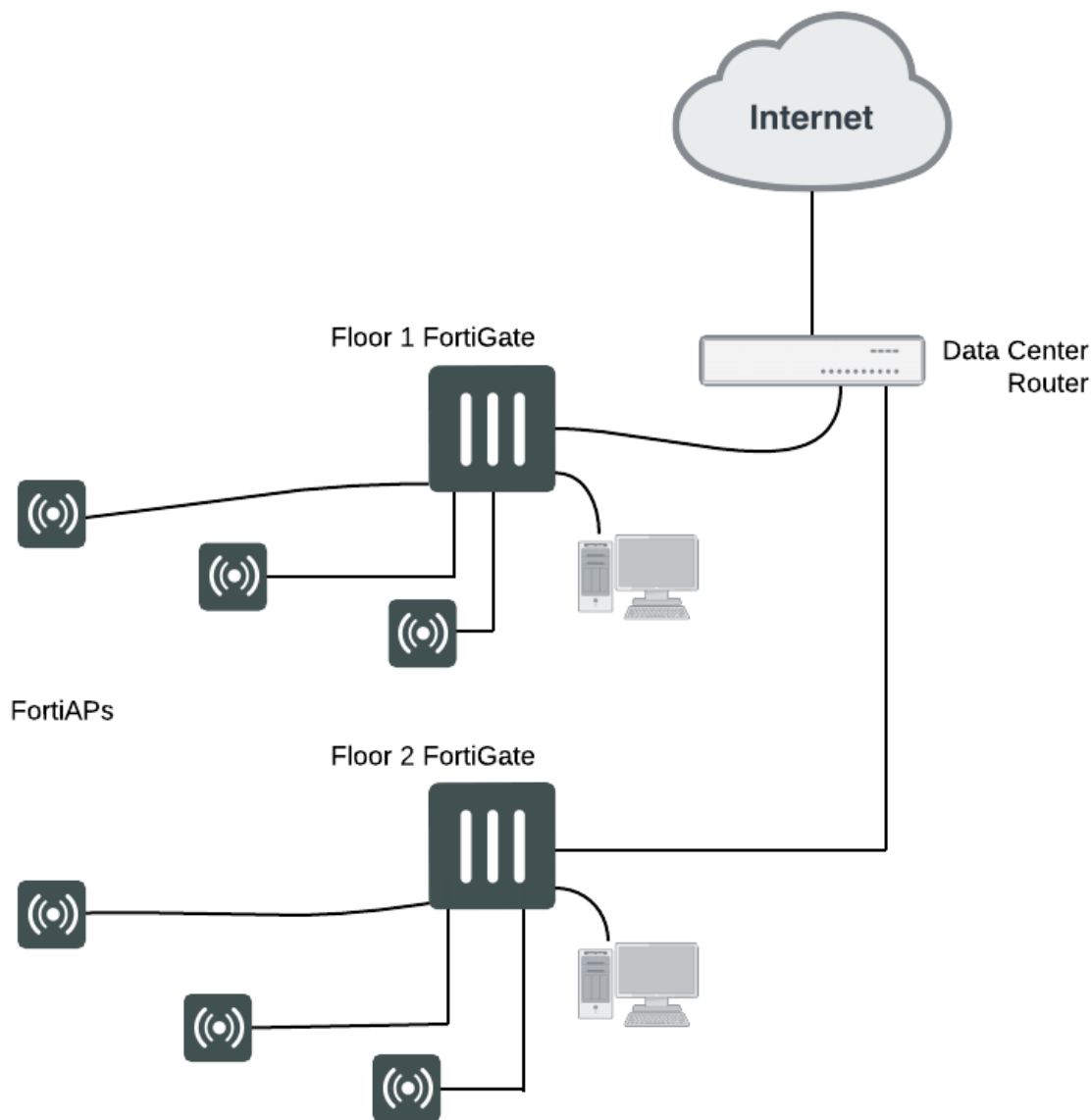
In most cases, FortiAP units can find WiFi controllers through the wired Ethernet without any special configuration. Review the following section, [Access point deployment on page 54](#), to make sure that your method of connecting the FortiAP unit to the WiFi controller is valid. Then, you are ready to follow the procedures in [Access point deployment on page 54](#).

If your FortiAP units are unable to find the WiFi controller, refer to [Access point deployment on page 54](#) for detailed information about the FortiAP unit's controller discovery methods and how you can configure them.

## Network topology for managed APs

The FortiAP unit can be connected to the FortiGate unit in any of the following ways:

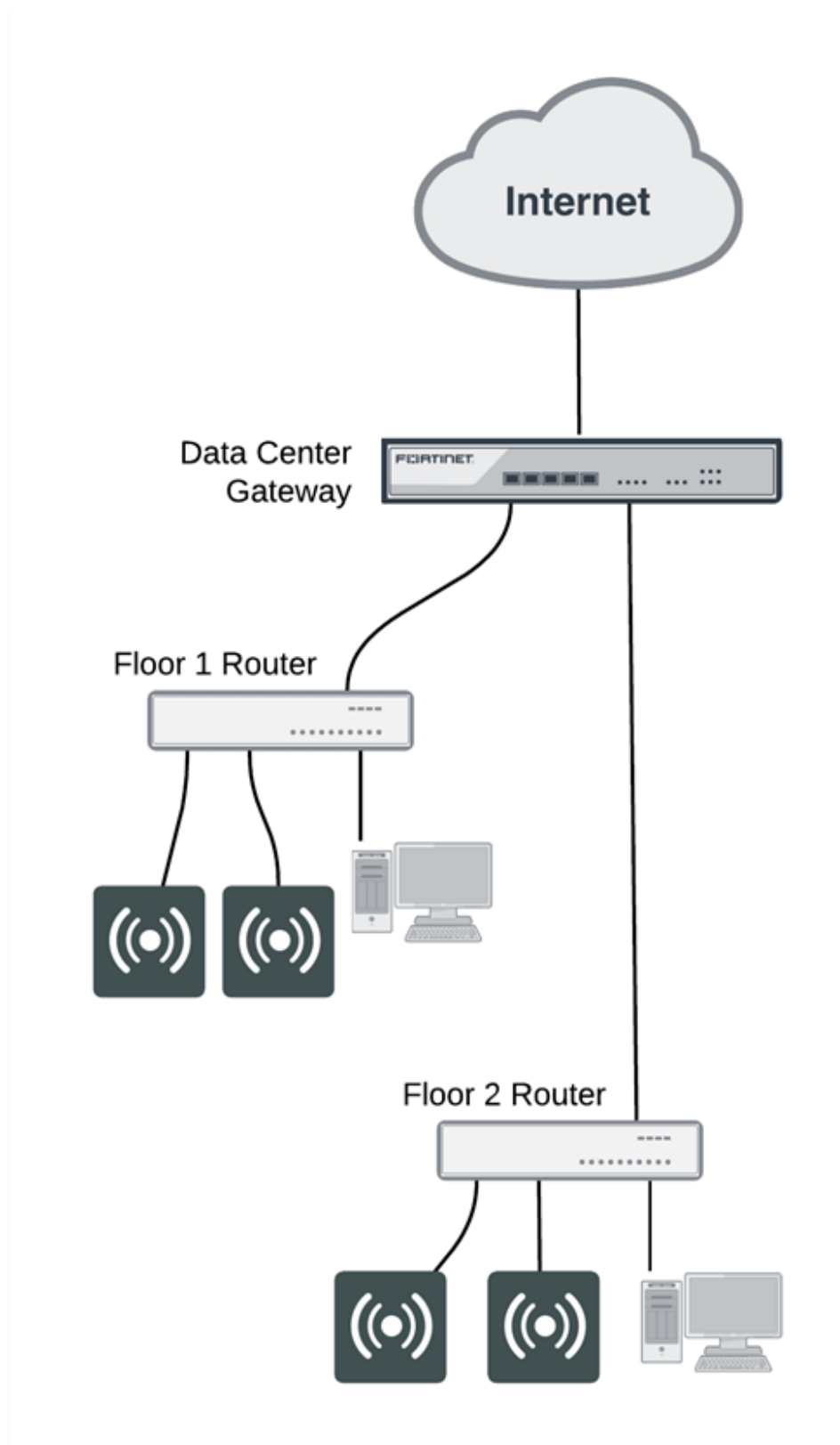
**Direct connection:** The FortiAP unit is directly connected to the FortiGate unit with no switches between them. This configuration is common for locations where the number of FortiAP's matches up with the number of 'internal' ports available on the FortiGate. In this configuration the FortiAP unit requests an IP address from the FortiGate unit, enters discovery mode and should quickly find the FortiGate WiFi controller. This is also known as a wirecloset deployment. See "Wirecloset and Gateway deployments" below.

**Wirecloset deployment**

**Switched Connection:** The FortiAP unit is connected to the FortiGate WiFi controller by an Ethernet switch operating in L2 switching mode or L3 routing mode. There must be a routable path between the FortiAP unit and the FortiGate unit and ports 5246 and 5247 must be open. This is also known as a gateway deployment. See Gateway Deployment below.

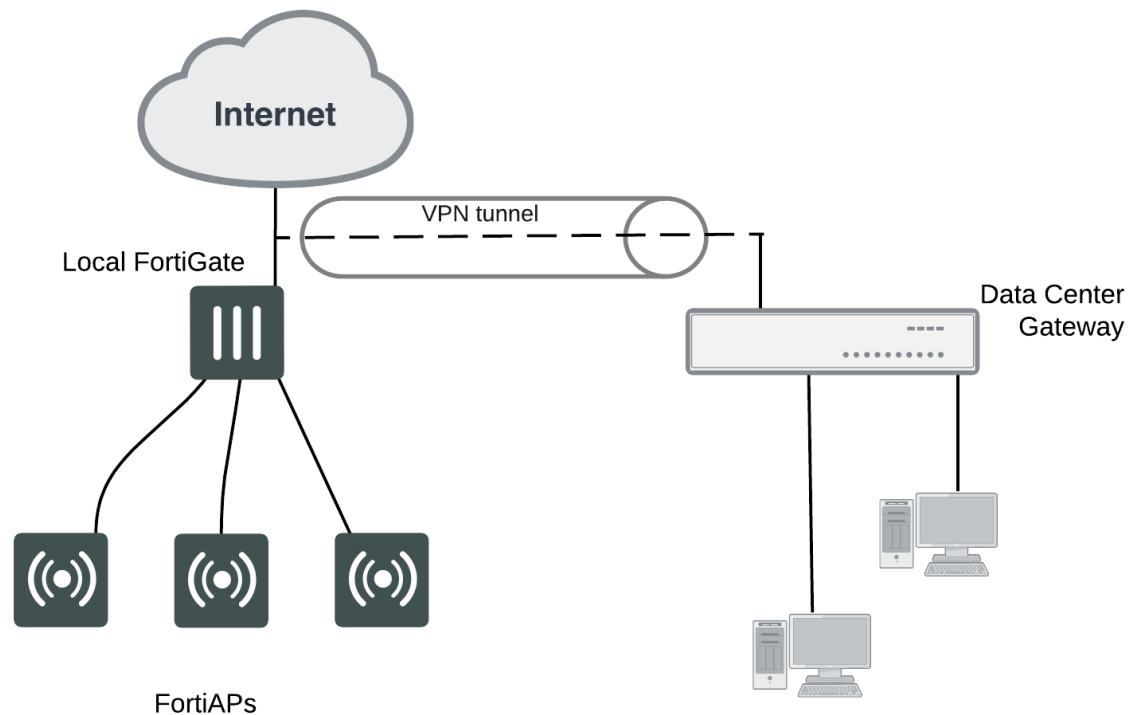
## **Gateway Deployment**





**Connection over WAN:** The FortiGate WiFi controller is off-premises and connected by a VPN tunnel to a local FortiGate. In this method of connectivity its best to configure each FortiAP with the static IP address of the WiFi controller. Each FortiAP can be configured with three WiFi controller IP addresses for redundant failover. This is also known as a datacenter remote management deployment. See Remote deployment below.

### Remote deployment



## Discovering and authorizing APs

After you prepare your FortiGate, you can connect your APs to discover them using the discovery methods described earlier. To prepare the FortiGate, you need to

- Configure the network interface to which the AP will connect.
- Configure DHCP service on the interface to which the AP will connect.
- Optionally, preauthorize FortiAP units. They will begin to function when connected.
- Connect the AP units and let the FortiGate unit discover them.
- Enable each discovered AP and configure it or assign it to an AP profile.

## Configuring the network interface for the AP unit

The interface to which you connect your wireless access point needs an IP address. No administrative access, DNS Query service or authentication should be enabled.

### To configure the interface for the AP unit - web-based manager

1. Go to **Network > Interfaces** and edit the interface to which the AP unit connects.
2. Set **Addressing Mode** to **Dedicate to Extension Device**.
3. Enter the IP address and netmask to use.  
This FortiGate unit automatically configures a DHCP server on the interface that will assign the remaining higher addresses up to .254 to FortiAP units. For example, if the IP address is 10.10.1.100, the FortiAP units will be assigned 10.10.1.101 to 10.10.1.254. To maximize the available addresses, use the .1 address for the interface: 10.10.1.1, for example.
4. Select **OK**.

### To configure the interface for the AP unit - CLI

In the CLI, you must configure the interface IP address and DHCP server separately.

```
config system interface
  edit port3
    set mode static
    set ip 10.10.70.1 255.255.255.0
  end
config system dhcp server
  edit 0
    set interface "dmz"
    config ip-range
      edit 1
        set end-ip 10.10.70.254
        set start-ip 10.10.70.2
      end
    set netmask 255.255.255.0
    set vci-match enable
    set vci-string "FortiAP"
  end
```

The optional `vci-match` and `vci-string` fields ensure that the DHCP server will provide IP addresses only to FortiAP units.

## Pre-authorizing a FortiAP unit

If you enter the FortiAP unit information in advance, it is authorized and will begin to function when it is connected.

### To pre-authorize a FortiAP unit

1. Go to **WiFi & Switch Controller > Managed FortiAPs** and select **Create New**.  
On some models the **WiFi Controller** menu is called **WiFi & Switch Controller**.
2. Enter the **Serial Number** of the FortiAP unit.
3. Configure the **Wireless Settings** as required.
4. Select **OK**.

## Enabling and configuring a discovered AP

Within two minutes of connecting the AP unit to the FortiGate unit, the discovered unit should be listed on **WiFi Controller > Managed FortiAPs** page. After you select the unit, you can authorize, edit or delete it.

### Discovered access point unit

+ Create New		Edit	Delete	Refresh	Authorize	AP Radio		Managed FortiAPs	0/32
Mesh	Access Point	State	Connected Via	SSIDs	Channel	Clients	OS Version	FortiAP Profile	
	FP221C3X14019926	?	192.168.2.2	Radio 1: Radio 2: Student-net	Radio1: 0 Radio2: 0	Radio 1: 0 Radio 2: 0		FAP221C-default	

When you authorize (enable) a FortiAP unit, it is configured by default to use the default FortiAP profile (determined by model). You can create and select a different profile if needed. The FortiAP profile defines the entire configuration for the AP.

### To add and configure the discovered AP unit - web-based manager

1. Go to **WiFi & Switch Controller > Managed FortiAPs**.  
This configuration also applies to local WiFi radio on FortiWiFi models.
2. Select the FortiAP unit from the list and edit it.
3. Optionally, enter a **Name**. Otherwise, the unit will be identified by serial number.
4. Select **Authorize**.
5. Select a **FortiAP Profile**.
6. Select **OK**.

The physical access point is now added to the system. If the rest of the configuration is complete, it should be possible to connect to the wireless network through the AP.

### To add the discovered AP unit - CLI

First get a list of the discovered access point unit serial numbers:

```
get wireless-controller wtp
```

Add a discovered unit and associate it with AP-profile1, for example:

```
config wireless-controller wtp
edit FAP22A3U10600118
set admin enable
set wtp-profile AP-profile1
end
```

### To view the status of the added AP unit

```
config wireless-controller wtp
edit FAP22A3U10600118
get
```

The `join-time` field should show a time, not "N/A". See the preceding web-based manager procedure for more information.

## Disable automatic discovery of unknown FortiAPs

By default, the FortiGate adds newly discovered FortiAPs to the Managed FortiAPs list, awaiting the administrator's authorization. Optionally, you can disable this automatic registration function to avoid adding unknown FortiAPs. A FortiAP will be registered and listed only if its serial number has already been added manually to the Managed FortiAPs list. AP registration is configured on each interface.

To disable automatic discovery and registration, enter the following command:

```
config system interface
  edit port15
    set ap-discover disable
  end
```

## Automatic authorization of extension devices

To simplify adding FortiAP or FortiSwitch devices to your network, you can enable automatic authorization of devices as they are connected, instead of authorizing each one individually.

This feature is only configurable in the CLI.

### To enable automatic authorization on all dedicated interfaces

```
config system global
  set auto-auth-extension-device enable
end
```

### To enable automatic authorization per-interface

```
config system interface
  edit <port>
    set auto-auth-extension-device enable
  end
```

## Assigning the same profile to multiple FortiAP units

The same profile can now be applied to multiple managed FortiAP units at the same time. To do this, do the following:

1. Go to **WiFi & Switch Controller > Managed FortiAPs** to view the AP list.
2. Select all FortiAP units you wish to apply the profile to.
3. Right click on one of the selected FortiAPs and select **Assign Profile**.
4. Choose the profile you wish to apply.

## Overriding the FortiAP profile

In the FortiAP configuration **WiFi & Switch Controller > Managed FortiAPs**, there several radio settings under **Override Radio 1** and **Override Radio 2** to choose a value independently of the FortiAP profile setting. When each of the radios are disabled, you will see what the FortiAP Profile has each of the settings configured to.

<b>Band</b>	The available options depend on the capability of the radio. Overriding <b>Band</b> also overrides <b>Channels</b> . Make appropriate settings in <b>Channels</b> .
<b>Channels</b>	Choose channels. The available channels depend on the Band.
<b>TX Power Control</b>	If you enable <b>Auto</b> , adjust to set the power range in dBm. If you enable <b>Manual</b> , adjust the slider. The 100% setting is the maximum power permitted in your region. See <a href="#">Configuring a WiFi LAN on page 29</a> .
<b>SSIDs</b>	Select between <b>Auto</b> or <b>Manual</b> . Selecting <b>Auto</b> eliminates the need to re-edit the profile when new SSIDs are created. However, you can still select SSIDs individually using <b>Manual</b> .

### To override radio settings in the CLI

In this example, Radio 1 is set to 802.11n on channel 11, regardless of the profile setting.

```
config wireless-controller wtp
edit FP221C3X14019926
config radio-1
set override-band enable
set band 802.11n
set override-channel enable
set channel 11
end
```

Override settings are available for band, channel, vaps (SSIDs), and txpower.

Outside of configuring radio settings, you can also override FortiAP LED state, WAN port mode, IP Fragmentation prevention method, spectrum analysis, split tunneling, and login password settings.

## Accessing the FortiAP CLI through the FortiGate unit

Enable remote login for the FortiAP. In the FortiAP Profile for this FortiAP, enable remote access.

## Connecting to the FortiAP CLI

The FortiAP unit has a CLI through which some configuration options can be set. You can access the CLI using Telnet.

### To access the FortiAP unit CLI through the FortiAP Ethernet port

1. Connect your computer to the FortiAP Ethernet interface, either directly with a cross-over cable or through a separate switch or hub.
2. Change your computer's IP address to 192.168.1.3
3. Telnet to IP address 192.168.1.2.  
Ensure that FortiAP is in a private network with no DHCP server for the static IP address to be accessible.
4. Login with user name admin and no password.
5. Enter commands as needed.
6. Optionally, use the `passwd` command to assign an administrative password for better security.
7. Save the configuration by entering the following command:

```
cfg -c .
```

8. Unplug the FortiAP and then plug it back in, in order for the configuration to take effect

## Accessing the FortiAP CLI through the FortiGate

After the FortiAP has been installed, physical access to the unit might be inconvenient. You can access a connected FortiAP unit's CLI through the FortiGate unit that controls it.

### To enable remote access to the FortiAP CLI

In the CLI, edit the FortiAP Profile that applies to this FortiAP.

```
config wireless-controller wtp-profile
edit FAP221C-default
set allowaccess telnet
end
```



FortiAP now supports HTTPS and SSH administrative access, as well as HTTP and Telnet. Use the command above to set administrative access to `telnet`, `http`, `https`, or `ssh`.

### To access the FortiAP unit CLI through the FortiGate unit - GUI

1. Go to **WiFi & Switch Controller > Managed FortiAPs**.
2. In the list, right-click the FortiAP unit and select **>\_Connect to CLI**.  
A detached Console window opens.
3. At the FortiAP login prompt, enter `admin`. When you are finished using the FortiAP CLI, enter `exit`.

### To access the FortiAP unit CLI through the FortiGate unit - CLI

1. Use the FortiGate CLI `execute telnet` command to access the FortiAP. For example, if the FortiAP unit IP address is 192.168.1.2, enter:  

```
execute telnet 192.168.1.2
```
2. At the FortiAP login prompt, enter `admin`. When you are finished using the FortiAP CLI, enter `exit`.



When a WiFi controller has taken control of the FortiAP unit, Telnet access to the FortiAP unit's CLI is no longer available.

## Checking and updating FortiAP unit firmware

You can view and update the FortiAP unit's firmware from the FortiGate unit that acts as its WiFi controller.

### Checking the FortiAP unit firmware version

Go to **WiFi & Switch Controller > Managed FortiAPs** to view the list of FortiAP units that the FortiGate unit can manage. The **OS Version** column shows the current firmware version running on each AP.

## Updating FortiAP firmware from the FortiGate unit

You can update the FortiAP firmware using either the web-based manager or the CLI. Only the CLI method can update all FortiAP units at once.

### To update FortiAP unit firmware - web-based manager

1. Go to **WiFi & Switch Controller > Managed FortiAPs**.
2. Right-click the FortiAP unit in the list and select **Upgrade Firmware**.  
or  
Edit the FortiAP entry and select **Upgrade from File** in **FortiAP OS Version**.
3. Select **Browse** and locate the firmware upgrade file.
4. Select **OK**.
5. When the upgrade process completes, select **OK**.  
The FortiAP unit restarts.

### To update FortiAP unit firmware - CLI

1. Upload the FortiAP image to the FortiGate unit.  
For example, the Firmware file is FAP\_22A\_v4.3.0\_b0212\_fortinet.out and the server IP address is 192.168.0.100.  

```
execute wireless-controller upload-wtp-image tftp FAP_22A_v4.3.0_b0212_fortinet.out 192.168.0.100
```

If your server is FTP, change `tftp` to `ftp`, and if necessary add your user name and password at the end of the command.

2. Verify that the image is uploaded:  

```
execute wireless-controller list-wtp-image
```
3. Upgrade the FortiAP units:  

```
exec wireless-controller reset-wtp all
```

If you want to upgrade only one FortiAP unit, enter its serial number instead of `all`.

## Updating FortiAP firmware from the FortiAP unit

You can connect to a FortiAP unit's internal CLI to update its firmware from a TFTP server on the same network. This method does not require access to the wireless controller.

1. Place the FortiAP firmware image on a TFTP server on your computer.
2. Connect the FortiAP unit to a separate private switch or hub or directly connect to your computer via a cross-over cable.
3. Change your computer's IP address to 192.168.1.3.
4. Telnet to IP address 192.168.1.2.  
This IP address is overwritten if the FortiAP is connected to a DHCP environment. Ensure that the FortiAP unit is in a private network with no DHCP server.
5. Login with the username "admin" and no password.
6. Enter the following command.  
For example, the FortiAP image file name is FAP\_22A\_v4.3.0\_b0212\_fortinet.out.  

```
restore FAP_22A_v4.3.0_b0212_fortinet.out 192.168.1.3
```



## Advanced WiFi controller discovery

A FortiAP unit can use any of six methods to locate a controller. By default, FortiAP units cycle through all six of the discovery methods. In most cases there is no need to make configuration changes on the FortiAP unit.

There are exceptions. The following section describes the WiFi controller discovery methods in more detail and provides information about configuration changes you might need to make so that discovery will work.

### Controller discovery methods

There are six methods that a FortiAP unit can use to discover a WiFi controller. Below is the list of AC discovery methods used in sequence, if the FortiAP's discovery type is set to auto:

**1(static) → 2(dhcp) → 3(dns) → 7(forticloud) → 5(multicast) → 6(broadcast)**

For every discovery type, FortiAP sends out discovery requests and sets a timer, an interval defined as a random number of seconds (between 2-180, default is 5 seconds), which is set via the CLI:

#### CLI syntax

```
config wireless-controller timers
  set discovery-interval 5
end
```

After the timeout is reached, FortiAP sends out another discovery request, up to a maximum of 3 times.

After about 3 - 15 seconds, if FortiAP has no AC connection, it will switch to another discovery type and repeat the above process until the last one (**broadcast**) fails, which will lead to SULKING state.

After about 30 seconds, FortiAP will go into an AC\_IP\_DISCOVER state. After the AC IP is found, it will go to IDLE state, and will eventually go to the DISCOVERY state, and repeat the above process again.

Note that, while the process above is showcasing the auto discovery method, it's recommended to set the AC\_DISCOVERY\_TYPE to your used method in order to reduce downtime.

### Static IP configuration

If FortiAP and the controller are not in the same subnet, broadcast and multicast packets cannot reach the controller. The admin can specify the controller's static IP on the AP unit. The AP unit sends a discovery request message in unicast to the controller. Routing must be properly configured in both directions.

#### To specify the controller's IP address on a FortiAP unit

```
cfg -a AC_IPADDR_1="192.168.0.100"
```

By default, the FortiAP unit receives its IP address, netmask, and gateway address by DHCP. If you prefer, you can assign these statically.

#### To assign a static IP address to the FortiAP unit

```
cfg -a ADDR_MODE=STATIC
cfg -a AP_IPADDR="192.168.0.100"
cfg -a AP_NETMASK="255.255.255.0"
cfg -a IPGW=192.168.0.1
cfg -c
```

For information about connecting to the FortiAP CLI, see [Connecting to the FortiAP CLI on page 62](#).

## DHCP

If you use DHCP to assign an IP address to your FortiAP unit, you can also provide the WiFi controller IP address at the same time. This is useful if the AP is located remotely from the WiFi controller and other discovery techniques will not work.

When you configure the DHCP server, configure Option 138 to specify the WiFi controller IP address. You need to convert the address into hexadecimal. Convert each octet value separately from left to right and concatenate them. For example, 192.168.0.1 converts to C0A80001.

If Option 138 is used for some other purpose on your network, you can use a different option number if you configure the AP units to match.

### To change the FortiAP DHCP option code

To use option code 139 for example, enter

```
cfg -a AC_DISCOVERY_DHCP_OPTION_CODE=139
```

For information about connecting to the FortiAP CLI, see [Connecting to the FortiAP CLI on page 62](#).

## DNS

The access point can discover controllers through your domain name server (DNS). For the access point to do so, you must configure your DNS to return controller IP addresses in response. Allow DNS lookup of the hostname configured in the AP by using the AP parameter "AC\_HOSTNAME\_1".

## FortiCloud

The access point can discover FortiCloud by doing a DNS lookup of the hardcoded FortiCloud AP controller hostname "apctrl1.fortinet.com". The forticloud AC discovery technique finds the AC info from apctrl1.fortinet.com using HTTPS.

**FortiCloud APController:** apctrl1.fortinet.com:443 208.91.113.187:443

## Broadcast request

The AP unit broadcasts a discovery request message to the network and the controller replies. The AP and the controller must be in the same broadcast domain. No configuration adjustments are required.

## Multicast request

The AP unit sends a multicast discovery request and the controller replies with a unicast discovery response message. The AP and the controller do not need to be in the same broadcast domain if multicast routing is properly configured.

The default multicast destination address is 224.0.1.140. It can be changed through the CLI. The address must be same on the controller and AP.

### To change the multicast address on the controller

```
config wireless-controller global
  set discovery-mc-addr 224.0.1.250
end
```

### To change the multicast address on a FortiAP unit

```
cfg -a AC_DISCOVERY_MC_ADDR="224.0.1.250"
```

For information about connecting to the FortiAP CLI, see [Advanced WiFi controller discovery on page 65](#).

## Wireless client load balancing for high-density deployments

Wireless load balancing allows your wireless network to distribute wireless traffic more efficiently among wireless access points and available frequency bands. FortiGate wireless controllers support the following types of client load balancing:

- Access Point Hand-off - the wireless controller signals a client to switch to another access point.
- Frequency Hand-off - the wireless controller monitors the usage of 2.4GHz and 5GHz bands, and signals clients to switch to the lesser-used frequency.

Load balancing is not applied to roaming clients.

### Access point hand-off

Access point handoff wireless load balancing involves the following:

- If the load on an access point (ap1) exceeds a threshold (of for example, 30 clients) then the client with the weakest signal will be signaled by wireless controller to drop off and join another nearby access point (ap2).
- When one or more access points are overloaded (for example, more than 30 clients) and a new client attempts to join a wireless network, the wireless controller selects the least busy access point that is closest to the new client and this access point is the one that responds to the client and the one that the client joins.

### Frequency hand-off or band-steering

Encouraging clients to use the 5GHz WiFi band if possible enables those clients to benefit from faster interference-free 5GHz communication. The remaining 2.4GHz clients benefit from reduced interference.

The WiFi controller probes clients to determine their WiFi band capability. It also records the RSSI (signal strength) for each client on each band.

If a new client attempts to join the network, the controller looks up that client's MAC address in its wireless device table and determines if it's a dual band device. If it is not a dual band device, then its allowed to join. If it is a dual band device, then its RSSI on 5GHz is used to determine whether the device is close enough to an access point to benefit from movement to 5GHz frequency.

If both conditions of 1) dual band device and 2) RSSI value is strong, then the wireless controller does not reply to the join request of the client. This forces the client to retry a few more times and then timeout and attempt to join the same SSID on 5GHz. Once the Controller see this new request on 5GHz, the RSSI is again measured and the client is allowed to join. If the RSSI is below threshold, then the device table is updated and the controller forces the client to timeout again. A client's second attempt to connect on 2.4GHz will be accepted.

## Configuration

From the web-based manager, edit a custom AP profile and select **Frequency Handoff** and **AP Handoff** as required for each radio on the AP.

From the CLI, you configure wireless client load balancing thresholds for each custom AP profile. Enable access point hand-off and frequency hand-off separately for each radio in the custom AP profile.

```
config wireless-controller wtp-profile
  edit new-ap-profile
    set handoff-rssi <rssi_int>
    set handoff-sta-thresh <clients_int>
    config radio-1
      set frequency-handoff {disable | enable}
      set ap-handoff {disable | enable}
    end
    config radio-2
      set frequency-handoff {disable | enable}
      set ap-handoff {disable | enable}
    end
  end
end
```

Where:

- `handoff-rssi` is the RSSI threshold. Clients with a 5 GHz RSSI threshold over this value are load balanced to the 5GHz frequency band. Default is 25. Range is 20 to 30.
- `handoff-sta-thresh` is the access point handoff threshold. If the access point has more clients than this threshold it is considered busy and clients are changed to another access point. Default is 30, range is 5 to 25.
- `frequency-handoff` enable or disable frequency handoff load balancing for this radio. Disabled by default.
- `ap-handoff` enable or disable access point handoff load balancing for this radio. Disabled by default.

Frequency handoff must be enabled on the 5GHz radio to learn client capability.

## FortiAP groups

FortiAP groups facilitate the application of FortiAP profiles to large numbers of FortiAPs. A FortiAP can belong to no more than one FortiAP group. A FortiAP group can include only one model of FortiAP.

Through the VLAN pool feature, a FortiAP group can be associated with a VLAN to which WiFi clients will be assigned. For more on VLAN pool assignment, see [VLAN assignment by VLAN pool](#).

FortiAP groups are only configurable in the CLI Console.

### To create a FortiAP group - CLI

In this example, `wtp-group-1` is created for a FortiAP-221C and one member device is added.

```
config wireless-controller wtp-group
  edit wtp-group-1
    set platform-type 221C
    config wtp-list
      edit FP221C3X14019926
    end
  end
end
```

## LAN port options

Some FortiAP models have one or more LAN interfaces that can provide wired network access. LAN ports can be

- bridged to the incoming WAN interface
- bridged to one of the WiFi SSIDs that the FortiAP unit carries
- connected by NAT to the incoming WAN interface

There are some differences among FortiAP models.

Models like 11C and 14C have one port labeled WAN and one or more ports labeled LAN. By default, the LAN ports are offline. You can configure LAN port operation in the FortiAP Profile in the GUI (**Wireless Controller > FortiAP Profiles**) or in the CLI (`config wireless-controller wtp-profile, config lan` subcommand).

Models like 320C, 320B, 112D, and 112B have two ports, labeled LAN1 and LAN2. LAN1 acts as a WAN port connecting the FortiAP to a FortiGate or FortiCloud. By default, LAN2 is bridged to LAN1. Other modes of LAN2 operation must be enabled in the CLI:

```
config wireless-controller wtp-profile
edit <profile_name>
set wan-port-mode wan-lan
end
```

By default `wan-port-mode` is set to `wan-only`.

When `wan-port-mode` is set to `wan-lan`, LAN2 Port options are available in the GUI and the CLI the same as the other FortiAP models that have labeled WAN and LAN ports.

## Bridging a LAN port with an SSID

Bridging a LAN port with a FortiAP SSID combines traffic from both sources to provide a single broadcast domain for wired and wireless users.

In this configuration

- The IP addresses for LAN clients come from the DHCP server that serves the wireless clients.
- Traffic from LAN clients is bridged to the SSID's VLAN. Dynamic VLAN assignment for hosts on the LAN port is not supported.
- Wireless and LAN clients are on the same network and can communicate locally, via the FortiAP.
- Any host connected to the LAN port will be taken as authenticated. RADIUS MAC authentication for hosts on the LAN port is not supported.

For configuration instructions, see [LAN port options on page 68](#).

## Bridging a LAN port with the WAN port

Bridging a LAN port with the WAN port enables the FortiAP unit to be used as a hub which is also an access point.

In this configuration

- The IP addresses for LAN clients come from the WAN directly and will typically be in the same range as the AP itself.
- All LAN client traffic is bridged directly to the WAN interface.
- Communication between wireless and LAN clients can only occur if a policy on the FortiGate unit allows it.

For configuration instructions, see [LAN port options on page 68](#).

## Configuring FortiAP LAN ports

You can configure FortiAP LAN ports for APs in a FortiAP Profile. A profile applies to APs that are the same model and share the same configuration. If you have multiple models or different configurations, you might need to create several FortiAP Profiles. For an individual AP, it is also possible to override the profile settings.

### To configure FortiAP LAN ports - web-based manager

1. If your FortiAP unit has LAN ports, but no port labeled WAN (models 320C, 320B, 112D, and 112B for example), enable LAN port options in the CLI:

```
config wireless-controller wtp-profile
  edit <profile_name>
    set wan-port-mode wan-lan
  end
```
2. Go to **WiFi & Switch Controller > FortiAP Profiles**.
3. Edit the default profile for your FortiAP model or select **Create New**.
4. If you are creating a new profile, enter a **Name** and select the correct **Platform** (model).
5. Select SSIDs.
6. In the **LAN Port** section, set **Mode** to **Bridge to** and select an SSID or **WAN Port** as needed. On some models with multiple LAN ports, you can set **Mode** to **Custom** and configure the LAN ports individually. Enable each port that you want to use and select an SSID or **WAN Port** as needed.
7. Select **OK**.

Be sure to select this profile when you authorize your FortiAP units.

### To configure FortiAP LAN ports - CLI

In this example, the default FortiAP-11C profile is configured to bridge the LAN port to the office SSID.

```
config wireless-controller wtp-profile
  edit FAP11C-default
    config lan
      set port-mode bridge-to-ssid
      set port-ssid office
    end
  end
end
```

In this example, the default FortiAP-28C profile is configured to bridge LAN port1 to the office SSID and to bridge the other LAN ports to the WAN port.

```
config wireless-controller wtp-profile
  edit FAP28C-default
    config lan
      set port1-mode bridge-to-ssid
      set port1-ssid office
      set port2-mode bridge-to-wan
      set port3-mode bridge-to-wan
      set port4-mode bridge-to-wan
      set port5-mode bridge-to-wan
      set port6-mode bridge-to-wan
      set port7-mode bridge-to-wan
      set port8-mode bridge-to-wan
    end
  end
end
```

In this example, the default FortiAP-320C profile is configured to bridge the LAN port to the office SSID.

```
config wireless-controller wtp-profile
  edit FAP320C-default
    set wan-port-mode wan-lan
    config lan
      set port-mode bridge-to-ssid
      set port-ssid office
    end
  end
end
```

### To configure FortiAP unit LAN ports as a FortiAP Profile override - web-based manager

1. Go to **WiFi & Switch Controller > Managed FortiAPs**.
2. Select the FortiAP unit from the list and select **Edit**.
3. Select the **FortiAP Profile**, if this has not already been done.
4. In the **LAN Port** section, select **Override**.  
The options for **Mode** are shown.
5. Set **Mode** to **Bridge to** and select an SSID or **WAN Port**, or **NAT to WAN** as needed.  
On some models with multiple LAN ports, you can set **Mode** to **Custom** and configure the LAN ports individually.  
Enable and configure each port that you want to use.
6. Select **OK**.

### To configure FortiAP unit LAN ports as a FortiAP Profile override - CLI

In this example, a FortiAP unit's configuration overrides the FortiAP Profile to bridge the LAN port to the office SSID.

```
config wireless-controller wtp
  edit FP320C3X14020000
    set wtp-profile FAP320C-default
    set override-wan-port-mode enable
    set wan-port-mode wan-lan
    set override-lan enable
    config lan
      set port-mode bridge-to-ssid
      set port-ssid office
    end
  end
end
```

## Preventing IP fragmentation of packets in CAPWAP tunnels

A common problem with controller-based WiFi networks is reduced performance due to IP fragmentation of the packets in the CAPWAP tunnel.

Fragmentation can occur because of CAPWAP tunnel overhead increasing packet size. If the original wireless client packets are close to the maximum transmission unit (MTU) size for the network (usually 1500 bytes for Ethernet networks unless jumbo frames are used) the resulting CAPWAP packets may be larger than the MTU, causing the packets to be fragmented. Fragmenting packets can result in data loss, jitter, and decreased throughput.

The FortiOS/FortiAP solution to this problem is to cause wireless clients to send smaller packets to FortiAP devices, resulting in 1500-byte CAPWAP packets and no fragmentation. The following options configure CAPWAP IP fragmentation control:

```
config wireless-controller wtp-profile
  edit FAP321C-default
    set ip-fragment-preventing {tcp-mss-adjust | icmp-unreachable}
    set tun-mtu-uplink {0 | 576 | 1500}
    set tun-mtu-downlink {0 | 576 | 1500}
  end
end
```

By default, `tcp-mss-adjust` is enabled, `icmp-unreachable` is disabled, and `tun-mtu-uplink` and `tun-mtu-downlink` are set to 0.

To set `tun-mtu-uplink` and `tun-mtu-downlink`, use the default TCP MTU value of 1500. This default configuration prevents packet fragmentation because the FortiAP unit limits the size of TCP packets received from wireless clients so the packets don't have to be fragmented before CAPWAP encapsulation.

The `tcp-mss-adjust` option causes the FortiAP unit to limit the maximum segment size (MSS) of TCP packets sent by wireless clients. The FortiAP does this by adding a reduced MSS value to the SYN packets sent by the FortiAP unit when negotiating with a wireless client to establish a session. This results in the wireless client sending packets that are smaller than the `tun-mtu-uplink` setting, so that when the CAPWAP headers are added, the CAPWAP packets have an MTU that matches the `tun-mtu-uplink` size.

The `icmp-unreachable` option affects all traffic (UDP and TCP) between wireless clients and the FortiAP unit. This option causes the FortiAP unit to drop packets that have the "Don't Fragment" bit set in their IP header and that are large enough to cause fragmentation and then send an ICMP packet -- type 3 "ICMP Destination unreachable" with code 4 "Fragmentation Needed and Don't Fragment was Set" back to the wireless controller. This should cause the wireless client to send smaller TCP and UDP packets.

## Overriding IP fragmentation settings on a FortiAP

If the FortiAP Profile settings for IP fragmentation are not appropriate for a particular FortiAP, you can override the settings on that specific unit.

```
config wireless-controller wtp
  edit FAP321C3X14019926
    set override-ip-fragment enable
    set ip-fragment-preventing {tcp-mss-adjust | icmp-unreachable}
    set tun-mtu-uplink {0 | 576 | 1500}
    set tun-mtu-downlink {0 | 576 | 1500}
  end
end
```

## LED options

Optionally, the status LEDs on the FortiAP can be kept dark. This is useful in dormitories, classrooms, hotels, medical clinics, hospitals where the lights might be distracting or annoying to occupants.

On the FortiGate, the LED state is controlled in the FortiAP Profile. By default the LEDs are enabled. The setting is CLI-only. For example, to disable the LEDs on FortiAP-221C units controlled by the FAP221C-default profile, enter:

```
config wireless-controller wtp-profile
```



```
edit FAP221C-default
  set led-state disable
end
```

You can override the FortiAP Profile LED state setting on an individual FortiAP using the CLI. For example, to make sure the LEDs are disabled on one specific unit, enter:

```
config wireless-controller wtp
  edit FAP221C3X14019926
    set override-led-state enable
    set led-state disable
  end
```

The LED state is also controllable from the FortiAP unit itself. By default, the FortiAP follows the FortiAP Profile setting.

## LED schedules

Use the command below (`led-schedule`) to assign recurring firewall schedules for illuminating LEDs on the FortiAP. This entry is only available when `led-state` is enabled, at which point LEDs will be visible when at least one of the schedules is valid.

Separate multiple schedule names with a space, as configured under `config firewall schedule group` and `config firewall schedule recurring`.

### Syntax

```
config wireless-controller wtp-profile
  edit {name}
    set led-state {enable | disable}
    set led-schedules <name>
  next
end
```

## CAPWAP bandwidth formula

The following section provides information on how to calculate the control plane CAPWAP traffic load in local bridging. The formula provided can help estimate the approximate package bandwidth cost. This is important for knowing precisely how much bandwidth is required on a WAN link for a centralized FortiGate managing hundreds of access points.

There are multiple factors that might affect the volume of CAPWAP control traffic, including the number of stations there are and large WiFi events.

The Ethernet/IP/UDP/CAPWAP uplink header cost should be approximately 66 bytes.

The tables below depict basic and commonly used optional CAPWAP bandwidth costs, on a per-AP basis.

Note the following:

- **STA:** The number of stations associated with the FortiAP.
- **ARP scan:** Finds hidden devices in your network.
- **VAP:** The number of VAPS held by the FortiAP.
- **Radio:** The number of radios (maximum of two) enabled by the FortiAP.

**Basic per-AP CAPWAP bandwidth costs**

Content	Time (seconds)	Payload (byte)	Package bandwidth cost (bps)
Echo Req	30	16	$(66+16)*8/30=21.86$
STA scan	30	$25+20*sta$	$(66+25+20*sta)*8/30=24.26+5.3*sta$
ARP scan	30	$25+18*sta$	$(66+25+18*sta)*8/30=24.26+4.8*sta$
STA CAP	30	$25+19*sta$	$(66+25+19*sta)*8/30=24.26+5.1*sta$
STA stats	1	$25+41*sta$	$(66+25+41*sta)*8/1=728.0+328.0*sta$
VAP stats	15	$40+18*vap$	$(66+40+18*vap)*8/15=56.53+9.6*vap$
Radio stats	15	$25+25*radio$	$(66+25+25*radio)*8/15=48.53+13.3*radio$
<b>Total:</b>			$908.7+343.2*sta+9.6*vap+13.3*radio$

**Commonly used optional per-AP CAPWAP bandwidth costs**

Content	Time (seconds)	Payload (byte)	Package bandwidth cost (bps)
AP scan	30	$25+63*scanned-ap$	$(66+25+63*scanned-ap)*8/30=24.26+16.8*scanned-ap$
<b>Total:</b>			$932.96+343.2*sta+9.6*vap+13.3*radio+16.8*scanned-ap$



Enabling WIDS features, LLDP, MESH, FortiPresence, and Client Station Locating Service can lead to additional bandwidth consumption.

**Example:**

There are 100 FortiAPs, with 187 stations distributed among them. Each FortiAP holds five VAPs among their radios, and each enables two radios. The basic CAPWAP bandwidth cost would be:

$$908.7*100+343.2*187+9.6*5*100+13.3*2*100 = \mathbf{162.51kbps}$$

Additionally, if two FortiAPs enabled "AP scan", and suppose one scans 99 APs in each scan and the other scans 20 APs in each scan, the additional CAPWAP bandwidth cost would be:

$$(24.26+16.8*99)+(24.26+16.8*20) = \mathbf{2\ kbps}$$

## Enabling LLDP protocol

You can enable the LLDP protocol in the FortiAP Profile via the CLI. Each FortiAP using that profile can then send back information about the switch and port that it is connected to.

To enable LLDP, enter the following:

```
config wireless-controller wtp-profile
  edit <profile-name>
    set lldp enable
  end
```

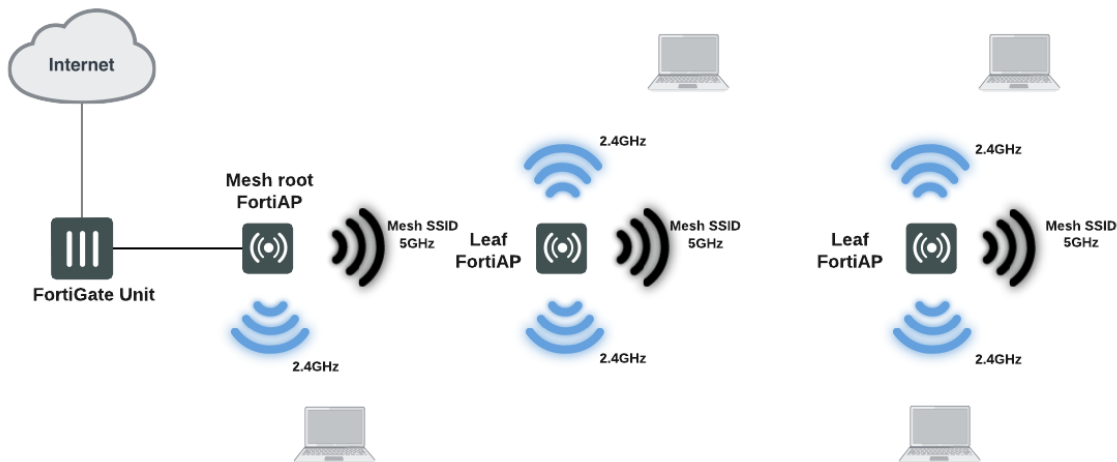
# Wireless mesh

The access points of a WiFi network are usually connected to the WiFi controller through Ethernet wiring. A wireless mesh eliminates the need for Ethernet wiring by connecting WiFi access points to the controller by radio. This is useful where installation of Ethernet wiring is impractical.

[Overview of wireless mesh](#)  
[Configuring a meshed WiFi network](#)  
[Configuring a point-to-point bridge](#)

## Overview of wireless mesh

The figure below shows a wireless mesh topology.



A wireless mesh is a multiple access point (AP) network in which only one FortiAP unit is connected to the wired network. The other FortiAPs communicate with the controller over a separate backhaul SSID that isn't available to regular WiFi clients. The AP connected to the network by Ethernet is called the mesh root node. The backhaul SSID carries CAPWAP discovery, configuration, and other communications that would usually be carried on an Ethernet connection.

The root node can be a FortiAP unit or the built-in AP of a FortiWiFi unit. APs that serve regular WiFi clients are called leaf nodes. Leaf APs also carry the mesh SSID for more distant leaf nodes. A leaf node can connect to the mesh SSID directly from the root node or from any of the other leaf nodes. This provides redundancy in case of an AP failure.

All access points in a wireless mesh configuration must have at least one of their radios configured to provide mesh backhaul communication. As with wired APs, when mesh APs start up, they can be discovered by a FortiGate or FortiWiFi unit WiFi controller and authorized to join the network.

The backhaul SSID delivers the best performance when it is carried on a dedicated radio. On a two-radio FortiAP unit, for example, the 5GHz radio could carry only the backhaul SSID while the 2.4GHz radio carries one or more SSIDs that serve users. You can configure background WiFi scanning in this mode.

The backhaul SSID can also share the same radio with SSIDs that serve users. Performance is reduced because the backhaul and user traffic compete for the available bandwidth. Background WiFi scanning isn't available in this mode. One advantage of this mode is that a two-radio AP can offer WiFi coverage on both bands.

## Wireless mesh deployment modes

There are two common wireless mesh deployment modes:

<b>Wireless mesh</b>	Access points are connected to a FortiGate or FortiWiFi unit WiFi controller. WiFi users connect to wireless SSIDs in the same way as on non-mesh WiFi networks.
<b>Wireless bridging</b>	Two LAN segments are connected together over a wireless link (the backhaul SSID). On the leaf AP, the Ethernet connection can be used to provide a wired network. Both WiFi and wired users on the leaf AP are connected to the LAN segment to which the root AP is connected.

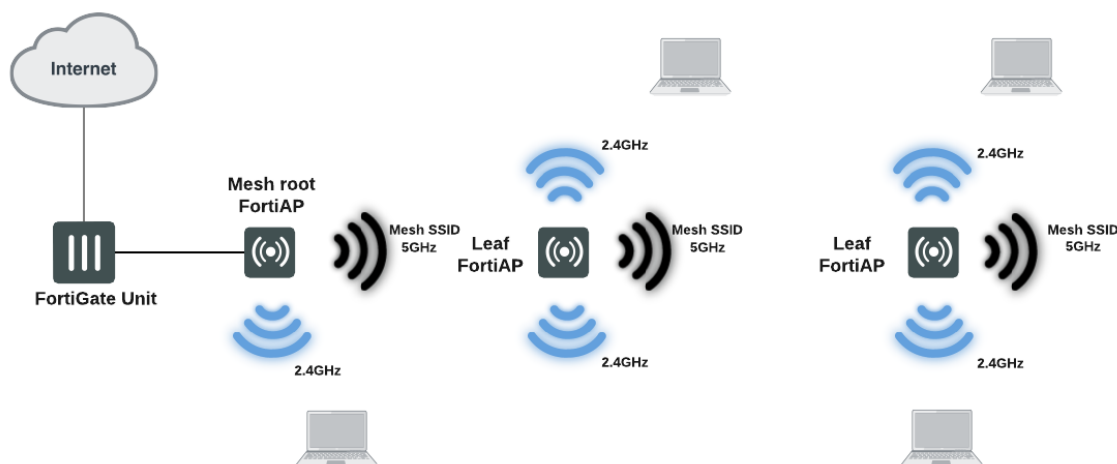
## Firmware requirements

All FortiAP units that are part of the wireless mesh network must be upgraded to FortiAP firmware version 5.0, build 003, or higher. FortiAP-222B units must have their BIOS upgraded to version 400012. The FortiWiFi or FortiGate unit used as the WiFi controller must be running FortiOS firmware version 5.0 or higher.

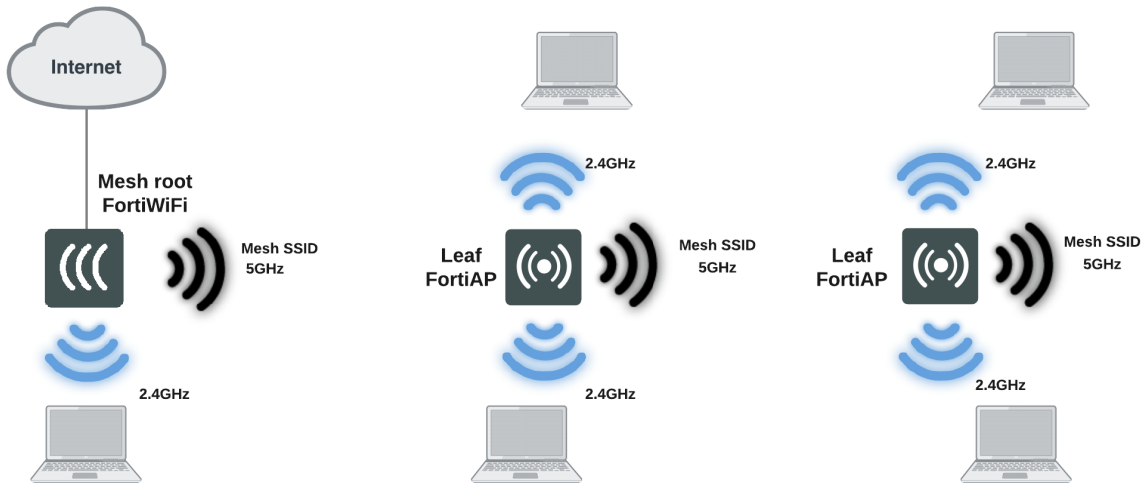
## Types of wireless mesh

A WiFi mesh can provide access to widely-distributed clients. The mesh root AP which is directly connected to the WiFi controller can be either a FortiAP unit or the built-in AP of a FortiWiFi unit that is also the WiFi controller.

### FortiAP units used as both mesh root AP and leaf AP

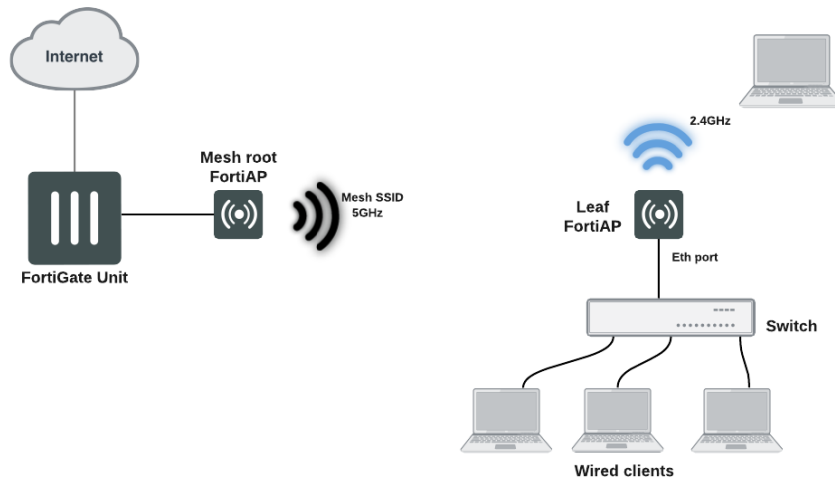


### FortiWiFi unit as mesh root AP with FortiAP units as leaf APs



An alternate use of the wireless mesh is as a point-to-point relay. Both wired and WiFi users on the leaf AP side are connected to the LAN segment on the mesh root side.

### Point-to-point wireless mesh



### Fast-roaming for mesh backhaul link

Mesh implementations for leaf FortiAP can perform background scanning when the leaf AP is associated with the root. Various options for background scanning can be configured with the CLI. See [Mesh variables on page 188](#) for more details.

## Configuring a meshed WiFi network

You need to:

- Create the mesh root SSID.
- Create the FortiAP profile.
- Configure mesh leaf AP units.
- Configure the mesh root AP, either a FortiWiFi unit's local radio or a FortiAP unit.
- Authorize the mesh leaf units when they connect to the WiFi Controller.
- Create security policies.

This section assumes that the end-user SSIDs already exist.

### Creating the mesh root SSID

The mesh route SSID is the radio backhaul that conveys the user SSID traffic to the leaf FortiAPs.

#### To configure the mesh root SSID

1. Go to **WiFi & Switch Controller > SSID** and select **Create New > SSID**.
2. Enter a **Name** for the WiFi interface.
3. In **Traffic Mode**, select **Mesh Downlink**.
4. Enter the **SSID**.
5. Set **Security Mode** to **WPA2 Personal** and enter the **Pre-shared key**.  
Remember the key, you need to enter it into the configurations of the leaf FortiAPs.
6. Select **OK**.

### Creating the FortiAP profile

Create a FortiAP profile for the meshed FortiAPs. If more than one FortiAP model is involved, you need to create a profile for each model. Typically, the profile is configured so that Radio 1 (5GHz) carries the mesh backhaul SSID while Radio 2 (2.4GHz) carries the SSIDs to which users connect.

For Radio 1, use the **Select SSIDs** option and choose only the backhaul SSID. The radio that carries the backhaul traffic must not carry other SSIDs.

Radio 2 carries user SSIDs and shouldn't carry the backhaul. Use the **Select SSIDs** option and choose the networks that you want to provide.

For more information, see [Configuring a WiFi LAN on page 29](#).

### Configuring the mesh root AP

The mesh root AP can be either a FortiWiFi unit's built-in AP or a FortiAP unit.

#### To enable a FortiWiFi unit's local radio as mesh root

1. On the FortiWiFi unit, go to **WiFi & Switch Controller > Local WiFi Radio**.
2. Select **Enable WiFi Radio**.

3. In **SSID**, select **Select SSIDs**, then select the mesh root SSID.
4. Optionally, adjust **Tx Power** or select **Auto Tx Power Control**.
5. Select **Apply**.



In a network with multiple wireless controllers, make sure that each mesh root has a unique SSID. Other controllers using the same mesh root SSID might be detected as fake or rogue APs. Go to **WiFi & Switch Controller > SSID** to change the SSID.

### To configure a network interface for the mesh root FortiAP unit

1. On the FortiGate unit, go to **Network > Interfaces**.
2. Edit the interface where you will connect the FortiAP unit.
3. Make sure that **Role** is **LAN**.
4. In **Addressing mode**, select **Dedicated to FortiSwitch**.
5. In **IP/Network Mask**, enter an IP address and netmask for the interface.  
DHCP will provide addresses to connected devices. To maximize the number of available addresses, the interface address should end with 1, for example 192.168.10.1.
6. Select **OK**.

At this point you can connect the mesh root FortiAP (see below). If you're going to configure leaf FortiAPs through the wireless controller (see "[Configuring a meshed WiFi network](#)" on page 79), connect the root unit later.

### To enable the root FortiAP unit

1. Connect the root FortiAP unit's Ethernet port to the FortiGate network interface that you configured.
2. On the FortiGate unit, go to **WiFi & Switch Controller > Managed FortiAPs**.  
If the root FortiAP unit isn't listed, wait 15 seconds and select **Refresh**. Repeat if necessary. If the unit is still missing after a minute or two, power cycle the root FortiAP unit and try again.
3. Right-click the FortiAP entry and choose your profile from the **Assign Profile** submenu.
4. Right-click the FortiAP entry and select **Authorize**.  
Initially, the **State** of the FortiAP unit is **Offline**. Periodically click **Refresh** to update the status. Within about two minutes, the state changes to **Online**.
5. Select **OK**.

## Configuring the mesh leaf FortiAPs

The FortiAP units that serve as leaf nodes must be preconfigured. This involves changing the FortiAP unit's internal configuration. You can do this by direct connection or through the FortiGate wireless controller.

### Method 1: Direct connection to the FortiAP

1. Configure the computer's IP as 192.168.1.3.
2. Connect the computer to the FortiAP unit's Ethernet port and use the default IP address, 192.168.1.2.
3. Log in to the FortiAP as admin. By default, no password is set.
4. Enter the following commands:
  - a. If you're using the GUI, go to **Connectivity > Uplink** and select the **Mesh** option. Then enter the **Mesh AP SSID** and **Mesh AP Password** (pre-shared key).



- b. If you're using the FortiAP CLI (Telnet or SSH), enter the following commands, substituting your own SSID and password (pre-shared key):

```
cfg -a MESH_AP_TYPE=1
cfg -a MESH_AP_SSID=fortinet.mesh.root
cfg -a MESH_AP_PASSWD=hardtoguess
cfg -c
exit
```

5. Disconnect the computer.
6. Power down the FortiAP.
7. Repeat the preceding steps for each leaf FortiAP.

## Method 2: Connecting through the FortiGate unit

1. Connect the Ethernet port on the leaf FortiAP to the FortiGate network interface that you configured for FortiAPs. Connect the FortiAP unit to a power source unless PoE is used.
2. On the FortiGate unit, go to **WiFi & Switch Controller > Managed FortiAPs**.  
If the FortiAP unit isn't listed, wait 15 seconds and select **Refresh**. Repeat if necessary. If the unit is still missing after a minute or two, power cycle the FortiAP unit and try again.
3. Select the discovered FortiAP unit and authorize it. Click **Refresh** every 10 seconds until the **State** indicator changes to **Online**.
4. Right-click the FortiAP and select **>\_Connect to CLI**. The **CLI Console** window opens. Log in as "admin".
5. Enter the following commands, substituting your own SSID and password (pre-shared key):

```
cfg -a MESH_AP_TYPE=1
cfg -a MESH_AP_SSID=fortinet.mesh.root
cfg -a MESH_AP_PASSWD=hardtoguess
cfg -c
exit
```
6. Disconnect the FortiAP and delete it from the **Managed FortiAP** list.
7. Repeat the preceding steps for each leaf FortiAP.

## Authorizing leaf APs

When the root FortiAP is connected and online, apply power to the preconfigured leaf FortiAPs. The leaf FortiAPs will connect themselves wirelessly to the WiFi Controller through the mesh network. You must authorize each unit.

1. On the FortiGate unit, go to **WiFi & Switch Controller > Managed FortiAPs**. Periodically select **Refresh** until the FortiAP unit is listed. This can take up to three minutes.  
The **State** of the FortiAP unit should be **Waiting for Authorization**.
2. Right-click the FortiAP entry and choose your profile from the **Assign Profile** submenu.
3. Right-click the FortiAP entry and select **Authorize**.  
Initially, the **State** of the FortiAP unit is **Offline**. Periodically click **Refresh** to update the status. Within about two minutes, the state changes to **Online**.

## Creating security policies

To permit traffic to flow from the end-user WiFi network to the network interfaces for the Internet and other networks, you need to create security policies and enable NAT. [\(cross reference for WiFi policy creation\)](#)

## Viewing the status of the mesh network

On the FortiGate unit, go to **WiFi & Switch Controller > Managed FortiAPs** to view the list of APs.

<a href="#">+ Create New</a>	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Refresh</a>	AP	Radio	Managed FortiAPs	2/32
Access Point	State	Connected Via	SSIDs	Channel	Clients	FortiAP Profile	
FP221C3X14019926	✓	192.168.2.3	Radio 1: example-staff Radio 2: fortinet.mesh.root	Radio1: 1 Radio2: 116	Radio 1: 0 Radio 2: 0	mesh-profile	
FP221C3X14023979	✓	192.168.2.2	Radio 1: example-staff Radio 2: fortinet.mesh.root	Radio1: 1 Radio2: 116	Radio 1: 0 Radio 2: 1	mesh-profile	

The **Connected Via** column lists the IP address of each FortiAP and uses icons to show whether the FortiAP is connected by Ethernet or mesh.

Ethernet	
Mesh	

To see how the FortiGate wireless controller connects to the FortiAP, mouse over the **Connected Via** information.

Connected Via	SSIDs
192.168.2.3	Radio 1: example-staff Radio 2: fortinet.mesh.root
192.168.2.2	Radio 1: example-staff Radio 2: fortinet.mesh.root

**AP Topology**

This FortiGate

...

FP221C3X14023979  
192.168.2.2

...

FP221C3X14019926  
192.168.2.3

## Configuring a point-to-point bridge

To connect two wired network segments using a WiFi link, you can create a point-to-point bridge. The effect is the same as connecting the two network segments to the same wired switch.

You need to:

- Configure a mesh-backhaul SSID and a mesh root AP as described in ["Configuring the mesh root AP" on page 79](#).  
**Note:** The mesh root AP for a point-to-point bridge must be a FortiAP unit, not the internal AP of a FortiWiFi unit.
- Configure a mesh leaf FortiAP as described in ["Configuring the mesh leaf FortiAPs" on page 80](#) and add these steps to configure the Ethernet bridge:

- If you're using the FortiAP web-based manager, select **Ethernet Bridge**
- If you're using the FortiAP CLI, insert the following command before the line reading `cfg -c`:  
`cfg -a MESH_ETH_BRIDGE=1`
- Connect the local wired network to the Ethernet port on the mesh leaf FortiAP unit. Users are assigned IP addresses from the DHCP server on the wired network connected to the mesh root FortiAP unit.



In general, the mesh-Ethernet bridge automatically detects VLAN ID tags in data packets and allows them to pass. When necessary, you can configure VLAN IDs for permanent support in a mesh-Ethernet bridge. To do this, enter the following commands in the mesh leaf FortiAP CLI:

```
cfg -a MESH_ETH_BRIDGE_VLANS=100,200,300
cfg -c
```

---

# Hotspot 2.0

Hotspot 2.0 Access Network Query Protocol (ANQP) is a query and response protocol that defines seamless roaming services offered by an AP. The following CLI commands are available under `config wireless-controller`, to configure Hotspot 2.0 ANQP.

## Syntax

```
config wireless-controller hotspot20 anqp-3gpp-cellular
edit {name}
    config mcc-mnc-list
    edit {id}
        set id {integer}
        set mcc {string}
        set mnc {string}
    next
next
end

config wireless-controller hotspot20 anqp-ip-address-type
edit {name}
    set ipv6-address-type {option}
    set ipv4-address-type {option}
next
end

config wireless-controller hotspot20 anqp-nai-realm
edit {name}
    config nai-list
    edit {name}
        set encoding {enable | disable}
        set nai-realm {string}
        config eap-method
        edit {index}
            set index {integer}
            set method {option}
            config auth-param
            edit {index}
                set index {integer}
                set id {option}
                set val {option}
            next
        next
    next
next
end

config wireless-controller hotspot20 anqp-network-auth-type
edit {name}
    set auth-type {option}
    set url {string}
next
end
```

```
config wireless-controller hotspot20 anqp-roaming-consortium
  edit {name}
    config oi-list
      edit {index}
        set index {integer}
        set oi {string}
        set comment {string}
      next
    next
  end
```

```
config wireless-controller hotspot20 anqp-venue-name
  edit {name}
    config value-list
      edit {index}
        set index {integer}
        set lang {string}
        set value {string}
      next
    next
  end
```

```
config wireless-controller hotspot20 h2qp-conn-capability
  edit {name}
    set icmp-port {option}
    set ftp-port {option}
    set ssh-port {option}
    set http-port {option}
    set tls-port {option}
    set pptp-vpn-port {option}
    set voip-tcp-port {option}
    set voip-udp-port {option}
    set ikev2-port {option}
    set ikev2-xx-port {option}
    set esp-port {option}
  next
end
```

```
config wireless-controller hotspot20 h2qp-operator-name
  edit {name}
    config value-list
      edit {index}
        set index {integer}
        set lang {string}
        set value {string}
      next
    next
  end
```

```
config wireless-controller hotspot20 h2qp-osu-provider
  edit {name}
    config friendly-name
      edit {index}
        set index {integer}
        set lang {string}
        set friendly-name {string}
      next
    next
  end
```

```

        next
        set server-uri {string}
        set osu-method {option}
        set osu-nai {string}
        config service-description
            edit {service-id}
                set service-id {integer}
                set lang {string}
                set service-description {string}
            next
        set icon {string}
    next
end

config wireless-controller hotspot20 h2qp-wan-metric
    edit {name}
        set link-status {option}
        set symmetric-wan-link {option}
        set link-at-capacity {enable | disable}
        set uplink-speed {integer}
        set downlink-speed {integer}
        set uplink-load {integer}
        set downlink-load {integer}
        set load-measurement-duration {integer}
    next
end

config wireless-controller hotspot20 hs-profile
    edit {name}
        set access-network-type {option}
        set access-network-internet {enable | disable}
        set access-network-asra {enable | disable}
        set access-network-esr {enable | disable}
        set access-network-uesa {enable | disable}
        set venue-group {option}
        set venue-type {option}
        set hessid {mac address}
        set proxy-arp {enable | disable}
        set l2tif {enable | disable}
        set pame-bi {enable | disable}
        set anqp-domain-id {integer}
        set domain-name {string}
        set osu-ssid {string}
        set gas-comeback-delay {integer}
        set gas-fragmentation-limit {integer}
        set dgaf {enable | disable}
        set deauth-request-timeout {integer}
        set wnm-sleep-mode {enable | disable}
        set bss-transition {enable | disable}
        set venue-name {string}
        set roaming-consortium {string}
        set nai-realm {string}
        set oper-friendly-name {string}
        config osu-provider
            edit {name}
                next
            set wan-metrics {string}
        end
    next
end

```

```
        set network-auth {string}
        set 3gpp-plmn {string}
        set conn-cap {string}
        set qos-map {string}
        set ip-addr-type {string}
    next
end

config wireless-controller hotspot20 icon
    edit {name}
        config icon-list
            edit {name}
                set lang {string}
                set file {string}
                set type {option}
                set width {integer}
                set height {integer}
            next
        next
    end

config wireless-controller hotspot20 qos-map
    edit {name}
        config dscp-except
            edit {index}
                set index
                set dscp
                set up
            next
        config dscp-range
            edit {index}
                set index
                set up
                set low
                set high
            next
        next
    end
```

# Combining WiFi and wired networks with a software switch

Combining WiFi and wired networks with a software switch

FortiAP local bridging (Private cloud-managed AP)

Using bridged FortiAPs to increase scalability

## Combining WiFi and wired networks with a software switch

A WiFi network can be combined with a wired LAN so that WiFi and wired clients are on the same subnet. This is a convenient configuration for users. Note that software switches are only available if your FortiGate is in Interface mode.



Wireless Mesh features cannot be used in conjunction with this configuration because they enable the FortiAP Local Bridge option.

To create the WiFi and wired LAN configuration, you need to:

- Configure the SSID so that traffic is tunneled to the WiFi controller.
- Configure a software switch interface on the FortiGate unit with the WiFi and internal network interface as members.
- Configure Captive Portal security for the software switch interface.

### To configure the SSID - web-based manager

1. Go to **WiFi & Switch Controller > SSID** and select **Create New**.
2. Enter:

<b>Interface name</b>	A name for the new WiFi interface, <code>homenet_if</code> for example.
<b>Traffic Mode</b>	Tunnel to Wireless Controller
<b>SSID</b>	The SSID visible to users, <code>homenet</code> for example.
<b>Security Mode</b> <b>Data Encryption</b> <b>Preshared Key</b>	Configure security as you would for a regular WiFi network.

3. Select **OK**.
4. Go to **WiFi & Switch Controller > Managed FortiAPs**, select the FortiAP unit for editing.
5. Authorize the FortiAP unit.  
The FortiAP unit can carry regular SSIDs in addition to the Bridge SSID.



### To configure the SSID - CLI

This example creates a WiFi interface "homenet\_if" with SSID "homenet" using WPA-Personal security, passphrase "Fortinet1".

```
config wireless-controller vap
  edit "homenet_if"
    set vdom "root"
    set ssid "homenet"
    set security wpa-personal
    set passphrase "Fortinet1"
  end
config wireless-controller wtp
  edit FAP22B3U11005354
    set admin enable
    set vaps "homenet_if"
  end
```

### To configure the FortiGate software switch - web-based manager

1. Go to **Network > Interfaces** and select **Create New > Interface**.
2. Enter:

<b>Interface Name</b>	A name for the new interface, <code>homenet_nw</code> for example.
<b>Type</b>	Software Switch
<b>Physical Interface Members</b>	Add <code>homenet_if</code> and the internal network interface.
<b>Addressing mode</b>	Select Manual and enter an address, for example <code>172.16.96.32/255.255.255.0</code>
<b>DHCP Server</b>	Enable and configure an address range for clients.
<b>Security Mode</b>	Select <b>Captive Portal</b> . Add the permitted <b>User Groups</b> .

3. Select **OK**.

### To configure the FortiGate unit - CLI

```
config system interface
  edit homenet_nw
    set ip 172.16.96.32 255.255.255.0
    set type switch
    set security-mode captive-portal
    set security-groups "Guest-group"
  end
config system interface
  edit homenet_nw
    set member "homenet_if" "internal"
  end
```

## VLAN configuration

If your environment uses VLAN tagging, you assign the SSID to a specific VLAN in the CLI. For example, to assign the `homenet_if` interface to VLAN 100, enter:

```
config wireless-controller vap
  edit "homenet_if"
    set vlanid 100
  end
```

## Additional configuration

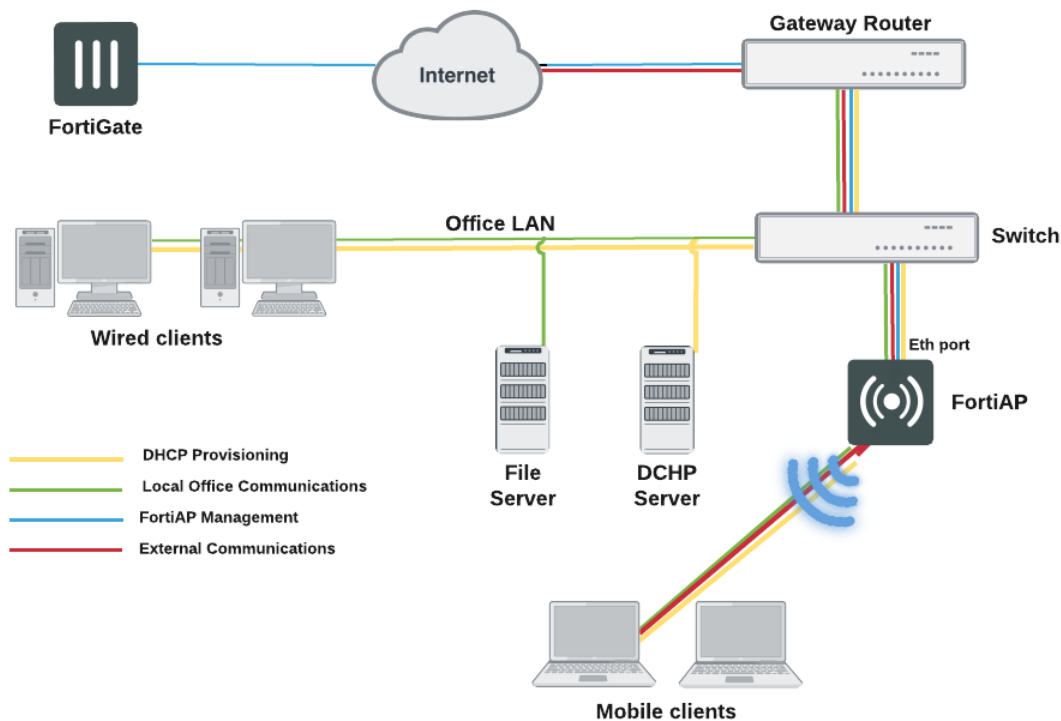
The configuration described above provides communication between WiFi and wired LAN users only. To provide access to other networks, create appropriate firewall policies between the software switch and other interfaces.

## FortiAP local bridging (Private cloud-managed AP)

A FortiAP unit can provide WiFi access to a LAN, even when the wireless controller is located remotely. This configuration is useful for the following situations:

- Installations where the WiFi controller is remote and most of the traffic is local or uses the local Internet gateway
- Wireless-PCI compliance with remote WiFi controller
- Telecommuting, where the FortiAP unit has the WiFi controller IP address pre-configured and broadcasts the office SSID in the user's home or hotel room. In this case, data is sent in the wireless tunnel across the Internet to the office and you should enable encryption using DTLS.

## Remotely-managed FortiAP providing WiFi access to local network



On the remote FortiGate wireless controller, the WiFi SSID is created with the **Bridge with FortiAP Interface** option selected. In this mode, no IP addresses are configured. The WiFi and Ethernet interfaces on the FortiAP behave as a switch. WiFi client devices obtain IP addresses from the same DHCP server as wired devices on the LAN.



The local bridge feature cannot be used in conjunction with Wireless Mesh features.

**Block-Intra-SSID Traffic** is available in Bridge mode. This is useful in hotspot deployments managed by a central FortiGate, but would also be useful in cloud deployments. Previously, this was only supported in Tunnel mode.

### To configure a FortiAP local bridge - web-based manager

1. Go to **WiFi & Switch Controller > SSID** and select **Create New > SSID**.
2. Enter:

<b>Interface name</b>	A name for the new WiFi interface.
<b>Traffic Mode</b>	Local bridge with FortiAP's Interface
<b>SSID</b>	The SSID visible to users.

**Security Mode**  
**Data Encryption**  
**Preshared Key**

Configure security as you would for a regular WiFi network.


3. Select **OK**.
4. Go to **WiFi & Switch Controller > Managed FortiAPs** and select the FortiAP unit for editing.
5. Authorize the FortiAP unit.  
 The FortiAP unit can carry regular SSIDs in addition to the Bridge SSID.

### SSID configured for local bridge operation

New Interface

Interface Name

Type

Traffic Mode 
 Local bridge with FortiAP's Int...


**WiFi Settings**

SSID

Security Mode

Pre-shared Key  (8 - 63 characters)

Allow New WiFi Client Connections When Controller Is Down ☐

Schedule 

Maximum Clients ☐

Optional VLAN ID

### To configure a FortiAP local bridge - CLI

This example creates a WiFi interface “branchbridge” with SSID “LANbridge” using WPA-Personal security, passphrase “Fortinet1”.

```
config wireless-controller vap
  edit "branchbridge"
    set vdom "root"
    set ssid "LANbridge"
    set local-bridging enable
    set security wpa-personal
    set passphrase "Fortinet1"
  end
config wireless-controller wtp
  edit FAP22B3U11005354
    set admin enable
    set vaps "branchbridge"
  end
```

Note that:



- Disabling `local-bridging` forcefully disables `local-standalone`. Also, disabling either `local-bridging` or `local-standalone` forcefully disables `intra-vap-privacy`.
- Enabling `intra-vap-privacy` forcefully disables `local-standalone`.
- Enabling `local-standalone` forcefully enables `local-bridging` also.

## Continued FortiAP operation when WiFi controller connection is down

The wireless controller, or the connection to it, might occasionally become unavailable. During such an outage, clients already associated with a bridge mode FortiAP unit continue to have access to the WiFi and wired networks. Optionally, the FortiAP unit can also continue to authenticate users if the SSID meets these conditions:

- **Traffic Mode is Local bridge with FortiAP's Interface.**  
In this mode, the FortiAP unit does not send traffic back to the wireless controller.
- **Security Mode is WPA2 Personal.**  
These modes do not require the user database. In WPA2 Personal authentication, all clients use the same pre-shared key which is known to the FortiAP unit.
- **Allow New WiFi Client Connections When Controller is down** is enabled.  
This field is available only if the other conditions have been met.

The “LANbridge” SSID example would be configured like this in the CLI:

```
config wireless-controller vap
  edit "branchbridge"
    set vdom "root"
    set ssid "LANbridge"
    set local-bridging enable
    set security wpa-personal
    set passphrase "Fortinet1"
    set local-authentication enable
  end
```

## Using bridged FortiAPs to increase scalability

The FortiGate wireless controller can support more FortiAP units in local bridge mode than in the normal mode. But this is only true if you configure some of your FortiAP units to operate in remote mode, which supports only local bridge mode SSIDs.

The Managed FortiAP page (**WiFi & Switch Controller > Managed FortiAPs**) shows at the top right the current number of Managed FortiAPs and the maximum number that can be managed, “5/64” for example. The maximum number, however, is true only if all FortiAP units operate in remote mode. For more detailed information, consult the Maximum Values Table. For each FortiGate model, there are two maximum values for managed FortiAP units: the total number of FortiAPs and the number of FortiAPs that can operate in normal mode.

**To configure FortiAP units for remote mode operation**

1. Create at least one SSID with **Traffic Mode** set to **Local bridge with FortiAP's Interface**.
2. Create a custom AP profile that includes *only* local bridge SSIDs.
3. Configure each managed FortiAP unit to use the custom AP profile. You also need to set the FortiAP unit's `wtp-mode` to `remote`, which is possible only in the CLI. The following example uses the CLI both to set `wtp-mode` and select the custom AP profile:

```
config wireless-controller wtp
  edit FAP22B3U11005354
    set wtp-mode remote
    set wtp-profile 220B_bridge
  end
```

# Using remote WLAN FortiAPs

Remote WLAN FortiAP models enable you to provide a pre-configured WiFi access point to a remote or traveling employee. Once plugged in at home or in a hotel room, the FortiAP automatically discovers the enterprise FortiGate WiFi controller over the Internet and broadcasts the same wireless SSID used in the corporate office. Communication between the WiFi controller and the FortiAP is secure, eliminating the need for a VPN.

## Split tunneling

By default, all traffic from the remote FortiAP is sent to the FortiGate WiFi controller. If split tunneling is configured, only traffic destined for the corporate office networks is routed to the FortiGate. Other general Internet traffic is routed unencrypted through the local gateway. Split tunneling avoids loading the FortiGate with unnecessary traffic and allows direct access to local private networks at the location of the FortiAP even if the connection to the WiFi controller goes down.

By default, split tunneling options are not visible in the FortiGate GUI. You can make these options visible using the following CLI command:

```
config system settings
    set gui-fortiap-split-tunneling enable
end
```

Split tunneling is configured in **Managed FortiAPs**, **FortiAP Profiles**, and enabled in the **SSID**.

## Configuring the FortiGate for remote FortiAPs

This section assumes that you have already defined SSIDs and now want to make them available to remote FortiAPs.

- Create FortiAP profiles for the Remote LAN FortiAP models
- If split tunneling will be used
  - configure override split tunneling in Managed FortiAPs
  - enable Split Tunneling in the SSID
  - configure the split tunnel networks in the FortiAP profile

## Override Split tunneling

Go to **WiFi & Switch Controller > Managed FortiAPs** and edit your managed APs. When preconfiguring the AP to connect to your FortiGate WiFi controller, you can choose to override split tunneling, optionally including the local subnet of the FortiAP.

## Creating FortiAP profiles

If you were not already using Remote LAN FortiAP models, you will need to create FortiAP profiles for them. In the FortiAP profile, you specify the SSIDs that the FortiAP will broadcast. For more information, see ["Creating a FortiAP profile" on page 33](#).

## Configuring split tunneling - FortiGate GUI

Go to **WiFi & Switch Controller > SSID** and edit your SSID. In the **WiFi Settings** section, enable **Split Tunneling**.

Go to **WiFi Controller > FortiAP Profiles** and edit the FortiAP Profile(s) that apply to the AP types used in the WiFi network. In the **Split Tunneling** section, enable **Include Local Subnet** and **Split Tunneling Subnet(s)**, where you can enter a list all of the destination IP address ranges that should *not* be routed through the the FortiGate WiFi controller. Packets for these destinations will instead be routed through the remote gateway local to the FortiAP.

The list of split tunneling subnets includes public Internet destinations and private subnets local to the FortiAP. Split tunneling public Internet destinations reduces traffic through the FortiGate unit. Split tunneling local private subnets allows these networks to be accessible to the client behind the FortiAP. Otherwise, private network IP destinations are assumed to be behind the FortiGate WiFi controller.

## Configuring split tunneling - FortiGate CLI

In this example, split tunneling is configured on the example-ssid WiFi network. On FortiAP model 21D, traffic destined for the 192.168.x.x range will not be routed through the FortiGate WiFi controller. This private IP address range is typically used as a LAN by home routers.

```
config wireless-controller vap
  edit example-ssid
    set split-tunneling enable
  end

config wireless-controller wtp-profile
  edit FAP21D-default
    set split-tunneling-acl-local-ap-subnet enable
    config split-tunneling-acl
      edit 1
        set dest-ip 192.168.0.0 255.255.0.0
      end
    end
  end
```

To enter multiple subnets, create a split-tunneling-acl entry for each one.

## Overriding the split tunneling settings on a FortiAP

If the FortiAP Profile split tunneling settings are not appropriate for a particular FortiAP, you can override the settings on that unit.

```
config wireless-controller wtp
  edit FAP321C3X14019926
    set override-split-tunnel enable
    set split-tunneling-acl-local-ap-subnet enable
    config split-tunneling-acl
      edit 1
        set dest-ip 192.168.10.0 255.255.255.0
      end
    end
  end
```



## Configuring the FortiAP units

Prior to providing a Remote WLAN FortiAP unit to an employee, you need to preconfigure the AP to connect to your FortiGate WiFi controller.

### To pre-configure a FortiAP

1. Connect the FortiAP to the FortiGate unit.
2. Go to **WiFi & Switch Controller > Managed FortiAPs** and wait for the FortiAP to be listed. Click **Refresh** periodically to see the latest information. Note the **Connected Via** IP address.
3. Go to **Dashboard**. In the CLI Console, log into the FortiAP CLI.  
For example, if the IP address is 192.168.1.4, enter:  

```
exec telnet 192.168.1.4
```

**Enter *admin* at the login prompt. By default, no password is set.**
4. Enter the following commands to set the FortiGate WiFi controller IP address. This should be the FortiGate Internet-facing IP address, in this example 172.20.120.142.  

```
cfg -a AC_IPADDR_1=172.20.120.142
```

```
cfg -c
```
5. Enter *exit* to log out of the FortiAP CLI.

## Preauthorizing FortiAP units

By preauthorizing FortiAP units, you facilitate their automatic authorization on the network. Also, you can assign each unit a unique name, such as the employee's name, for easier tracking.

1. Go to **WiFi & Switch Controller > Managed FortiAPs** and create a new entry.
2. Enter the **Serial Number** of the FortiAP unit and give it a **Name**. Select the appropriate **FortiAP Profile**.
3. Click **OK**.

Repeat this process for each FortiAP.

# Features for high-density deployments

High-density environments such as auditoriums, classrooms, and meeting rooms present a challenge to WiFi providers. When a large number of mobile devices try to connect to a WiFi network, difficulties arise because of the limited number of radio channels and interference between devices.

FortiOS and FortiAP devices provide several tools to mitigate the difficulties of high-density environments.

## Multiple FortiAP firmware upgrades at once

Administrators can configure multiple FortiAP and FortiSwitch firmware upgrades to occur in one click (under **WiFi & Switch Controller > Managed FortiAPs**), removing the need to upgrade each device one at a time.

## Power save feature

Occasionally, voice calls can become disrupted. One way to alleviate this issue is by controlling the power save feature, or to disable it altogether.

Manually configure packet transmit optimization settings by entering the following command:

```
config wireless-controller wtp-profile
edit <name>
    config <radio-1> | <radio-2>
        set transmit-optimize {disable | power-save | aggr-limit | retry-limit | sendbar}
```

- **disable:** Disable transmit optimization.
- **power-save:** Mark a client as power save mode if excessive transmit retries happen.
- **aggr-limit:** Set aggregation limit to a lower value when data rate is low.
- **retry-limit:** Set software retry limit to a lower value when data rate is low.
- **send-bar:** Do not send BAR frame too often.

## 11n radio powersave optimization

The following `powersave-optimize` parameters (under `config radio`) are used for 11n radios to optimize system performance for specific situations.

- **tim:** Set traffic indication map (TIM) bit for client in power save mode. TIM bit mask indicates to any sleeping listening stations if the AP has any buffered frames present. If enabled, the AP will always indicate to the connected client that there is a packet waiting in the AP, so it will help to prevent the client from entering a sleep state.
- **ac-vo:** Use Access Category (AC) Voice (VO) priority to send packets in the power save queue. AC VO is one of the highest classes/priority levels used to ensure quality of service (QoS). If enabled, when a client returns from a sleep state, the AP will send its buffered packet using a higher priority queue, instead of the normal priority queue.
- **no-obss-scan:** Do not put Overlapping Basic Service Set (OBSS), or high-noise (i.e. non-802.11), scan IE into a Beacon or Probe Response frame.
- **no-11b-rate:** Do not send frame using 11b data rate.

- **client-rate-follow:** Adapt transmitting PHY rate with receiving PHY rate from client. If enabled, the AP will integrate the current client's transmission PHY rate into its rate adaptation algorithm for transmitting.

## Broadcast packet suppression

You can use broadcast packet suppression to reduce the traffic on your WiFi networks. In addition, some broadcast packets are unnecessary or even potentially detrimental to the network and should be suppressed. To configure broadcast suppression for each virtual access point, enter the following commands:

```
config wireless-controller vap
  edit <name>
    set broadcast-suppression {dhcp-up | dhcp-down | dhcp-starvation | arp-known | arp-unknown | arp-reply | arp-poison | arp-proxy | netbios-ns | netbios-ds | ipv6 | all-other-mc | all-other-bc}
  end
```

Option	Description
dhcp-up	Suppress DHCP discovery and request packets broadcast by WiFi clients. Forward DHCP packets to the Ethernet uplink only. Prevent malicious WiFi clients from acting as DHCP servers. Default setting.
dhcp-down	Suppress DHCP packets broadcast by the Ethernet downlink to WiFi clients. Prevent malicious WiFi clients from acting as DHCP servers.
dhcp-starvation	Suppress DHCP starvation attacks from malicious WiFi clients. Prevent malicious WiFi clients from depleting the DHCP address pool.
arp-known	Suppress ARP request packets broadcast to known WiFi clients. Instead, forward ARP packets as unicast packets to the known clients. Default setting.
arp-unknown	Suppress ARP request packets broadcast to unknown WiFi clients.
arp-reply	Suppress ARP reply packets broadcast by WiFi clients. Instead, forward the ARP packets as unicast packets to the clients with target MAC addresses.
arp-poison	Suppress ARP poison attacks from malicious WiFi clients. Prevent malicious WiFi clients from spoofing ARP packets.
arp-proxy	<p>Suppress ARP request packets broadcast by the Ethernet downlink to known WiFi clients. Instead, send ARP reply packets to the Ethernet uplink, as a proxy for WiFi clients.</p> <p>The <code>arp-known</code> option must be set for <code>arp-proxy</code> to work.</p>
netbios-ns	Suppress NetBIOS name services packets with UDP port 137.
netbios-ds	Suppress NetBIOS datagram services packets with UDP port 138.

Option	Description
ipv6	Suppress IPv6 broadcast packets.
all-other-mc	Suppress multicast packets not covered by any of the specific options.
all-other-bc	Suppress broadcast packets not covered by any of the specific options.

The default configuration enables both the `dhcp-up` and `arp-known` options. The following example leaves the default settings in place and also configures a virtual access point to suppress:

- unnecessary DHCP down link broadcast packets
- broadcast ARP requests for unknown WiFi clients
- other broadcast packets not specifically identified

```
config wireless-controller vap
  edit <name>
    set broadcast-suppression dhcp-up arp-known dhcp-down arp-unknown all-other-bc
  end
```

## Multicast to unicast conversion

FortiOS provides a multicast enhancement option (disabled by default) that converts multicast streams to unicast and improves performance in WiFi networks. Multicast data, such as streaming audio or video, is sent at a low data rate in WiFi networks. A unicast stream is sent to each client at high data rate that makes more efficient use of air time. To enable multicast-to-unicast conversion, enter the following commands:

```
config wireless-controller vap
  edit <vap_name>
    set multicast-enhance enable
  end
```

## Ignore weak or distant clients

Clients beyond the intended coverage area can have some impact on your high-density network. Your APs will respond to these clients' probe signals, consuming valuable air time. You can configure your WiFi network to ignore weak signals that most likely come from beyond the intended coverage area. The settings are available in the CLI:

```
config wireless-controller vap
  edit <vap_name>
    set probe-resp-suppression enable
    set probe-resp-threshold <level_int>
  end
```

**vap\_name** is the SSID name.

**probe-resp-threshold** is the signal strength in dBm below which the client is ignored. The range is -95 to -20dBm. The default level is -80dBm.

## Turn off the 802.11b protocol

By disabling support for the obsolete 802.11b protocol, you can reduce the air time that data frames occupy. These signals will now be sent at a minimum of 6Mbps, instead of 1Mbps. You can set this for each radio in the FortiAP profile, using the CLI:

```
config wireless-controller wtp-profile
  edit <name_string>
    config radio-1
      set powersave-optimize no-11b-rate
    end
```

## Disable low data rates

Each of the 802.11 protocols supports several data rates. By disabling the lowest rates, air time is conserved, allowing the channel to serve more users. You can set the available rates for each 802.11 protocol: a, b, g, n, ac. Data rates set as Basic are mandatory for clients to support. Other specified rates are supported.

The 802.11 a, b, and g protocols are specified by data rate. 802.11a can support 6,9,12, 18, 24, 36, 48, and 54 Mb/s. 802.11b/g can support 1, 2, 5.5, 6, 9,12, 18, 24, 36, 48, 54 Mb/s. Basic rates are specified with the suffix "basic", "12-basic" for example. The capabilities of expected client devices need to be considered when deciding the lowest Basic rate.

The 802.11n and ac protocols are specified by the Modulation and Coding Scheme (MCS) Index and the number of spatial streams.

- 802.11n with 1 or 2 spatial streams can support mcs0/1, mcs1/1, mcs2/1, mcs3/1, mcs4/1, mcs5/1, mcs6/1, mcs7/1, mcs8/2, mcs9/2, mcs10/2, mcs11/2, mcs12/2, mcs13/2, mcs14/2, mcs15/2.
- 802.11n with 3 or 4 spatial streams can support mcs16/3, mcs17/3, mcs18/3, mcs19/3, mcs20/3, mcs21/3, mcs22/3, mcs23/3, mcs24/4, mcs25/4, mcs26/4, mcs27/4, mcs28/4, mcs29/4, mcs30/4, mcs31/4.
- 802.11ac with 1 or 2 spatial streams can support mcs0/1, mcs1/1, mcs2/1, mcs3/1, mcs4/1, mcs5/1, mcs6/1, mcs7/1, mcs8/1, mcs9/1, mcs0/2, mcs1/2, mcs2/2, mcs3/2, mcs4/2, mcs5/2, mcs6/2, mcs7/2, mcs8/2, mcs9/2.
- 802.11ac with 3 or 4 spatial streams can support mcs0/3, mcs1/3, mcs2/3, mcs3/3, mcs4/3, mcs5/3, mcs6/3, mcs7/3, mcs8/3, mcs9/3, mcs0/4, mcs1/4, mcs2/4, mcs3/4, mcs4/4, mcs5/4, mcs6/4, mcs7/4, mcs8/4, mcs9/4

Here are some examples of setting basic and supported rates.

```
config wireless-controller vap
  edit <vap_name>
    set rates-11a 12-basic 18 24 36 48 54
    set rates-11bg 12-basic 18 24 36 48 54
    set rates-11n-ss34 mcs16/3 mcs18/3 mcs20/3 mcs21/3 mcs22/3 mcs23/3 mcs24/4 mcs25/4
    set rates-11ac-ss34 mcs0/3 mcs1/3 mcs2/3 mcs9/4 mcs9/3
  end
```

## Limit power

High-density deployments usually cover a small area that has many clients. Maximum AP signal power is usually not required. Reducing the power reduces interference between APs. Fortinet recommends that you use FortiAP

automatic power control. You can set this in the FortiAP profile.

1. Go to **WiFi & Switch Controller > FortiAP Profiles** and edit the profile for your AP model.
2. For each radio, enable **Auto TX Power Control** and set the **TX Power Low** and **TX Power High** levels. The default range of 10 to 17dBm is recommended.

## Use frequency band load-balancing

In a high-density environment is important to make the best use of the two WiFi bands, 2.4GHz and 5GHz. The 5GHz band has more non-overlapping channels and receives less interference from non-WiFi devices, but not all devices support it. Clients that are capable of 5GHz operation should be encouraged to use 5GHz rather than the 2.4GHz band.

To load-balance the WiFi bands, you enable Frequency Handoff in the FortiAP profile. In the FortiGate web-based manager, go to **WiFi & Switch Controller > FortiAP Profiles** and edit the relevant profile. Or, you can use the CLI:

```
config wireless-controller wtp-profile
  edit FAP221C-default
    config radio-1
      set frequency-handoff enable
    end
```

The FortiGate WiFi controller continuously performs a scan of all clients in the area and records their signal strength (RSSI) on each band. When Frequency Handoff is enabled, the AP does not reply to clients on the 2.4GHz band that have sufficient signal strength on the 5GHz band. These clients can associate only on the 5GHz band. Devices that support only 2.4GHz receive replies and associate with the AP on the 2.4GHz band.

## Setting the handoff RSSI threshold

The FortiAP applies load balancing to a client only if the client has a sufficient signal level on 5GHz. The minimum signal strength threshold is set in the FortiAP profile, but is accessible only through the CLI:

```
config wireless-controller wtp-profile
  edit FAP221C-default
    set handoff-rssi 25
  end
```

`handoff-rssi` has a range of 20 to 30. RSSI is a relative measure. The higher the number, the stronger the signal.

## AP load balancing

The performance of an AP is degraded if it attempts to serve too many clients. In high-density environments, multiple access points are deployed with some overlap in their coverage areas. The WiFi controller can manage the association of new clients with APs to prevent overloading.

To load-balance between APs, enable AP Handoff in the FortiAP profile. In the FortiGate web-based manager, go to **WiFi & Switch Controller > FortiAP Profiles** and edit the relevant profile. Or, you can use the CLI:

```
config wireless-controller wtp-profile
  edit FAP221C-default
```

```
config radio-1
    set ap-handoff enable
end
```

When an AP exceeds the threshold (the default is 30 clients), the overloaded AP does not reply to a new client that has a sufficient signal at another AP.

## Setting the AP load balance threshold

The thresholds for AP handoff are set in the FortiAP profile, but is accessible only through the CLI:

```
config wireless-controller wtp-profile
    edit FAP221C-default
        set handoff-sta-thresh 30
        set handoff-rssi 25
    end
```

`handoff-sta-thresh` sets the number of clients at which AP load balancing begins. It has a range of 5 to 35.

`handoff-rssi` Sets the minimum signal strength that a new client must have at an alternate AP for the overloaded AP to ignore the client. It has a range of 20 to 30. RSSI is a relative measure. The higher the number, the stronger the signal.

## Application rate-limiting

To prevent particular application types from consuming too much bandwidth, you can use the FortiOS Application Control feature.

1. Go to **Security Profiles > Application Control**.  
You can use the default profile or create a new one.
2. Click the category, select **Traffic Shaping** and then select the priority for the category.  
Repeat for each category to be controlled.
3. Select **Apply**.
4. Go to **Policy & Objects > IPv4 Policy** and edit your WiFi security policy.
5. In **Security Profiles**, set **Application Control** ON and select the security profile that you edited.
6. Select **OK**.

## AP group management and dynamic VLAN assignment

The FortiGate can create FortiAP Groups, under **WiFi & Switch Controller > Managed FortiAPs** by selecting **Create New > Managed AP Group**, where multiple APs can be managed. AP grouping allows specific profile settings to be applied to many APs all at once that belong to a certain AP group, simplifying the administrative workload.

Note that each AP can only belong to one group.

In addition, VLANs can be assigned dynamically based on the group which an AP belongs. When defining an SSID, under **WiFi & Switch Controller > SSID**, a setting called **VLAN Pooling** can be enabled where you can either assign the VLAN ID of the AP group the device is connected to, to each device as it is detected, or to

always assign the same VLAN ID to a specific device. Dynamic VLAN assignment allows the same SSID to be deployed to many APs, avoiding the need to produce multiple SSIDs.

## Sharing tunnel SSIDs within a single managed AP between VDOMs as a virtual AP for multi-tenancy

This feature provides the ability to move a tunnel mode VAP into a VDOM, similar to an interface/VLAN in VDOMs. FortiAP is registered into the root VDOM.

Within a customer VDOM, customer VAPs can be created/added. In the root VDOM, the customer VAP can be added to the registered FortiAP. Any necessary firewall rules and interfaces can be configured between the two VDOMs.

### Syntax

```
config wireless-controller global
  set wtp-share {enable | disable}
end
```

## Manual quarantine of devices on FortiAP (tunnel mode)

Quarantined MAC addresses are blocked on the connected FortiAP from the network and the LAN. When a tunnel VAP is created, a sub-interface named **wqtn** is automatically created under tunnel interface. This sub-interface is added under a software switch.

To quarantine an SSID, go to **WiFi & Switch Controller > SSID**. Edit the SSID, and enable **Quarantine Host** is enabled under **WiFi Settings**.

Alternatively, this can be configured in the CLI Console. This feature consolidates previous CLI syntax for quarantining a host, so that the host does not need to be configured in multiple places (FortiAP and FortiSwitch). Host endpoints can be entered in a single place and the host will be quarantined throughout the access layer devices on the Fortinet Security Fabric.



Note that you can only an SSID in Tunnel Mode.

### Syntax - SSID:

```
config wireless-controller vap
  edit <name>
    set quarantine {enable | disable}
  next
end
```

### Syntax - Software Switch, DHCP, and User Quarantine

```
config system switch-interface
  edit "wqt.root"
```



```
        set vdom "root"
        set member "wqtn.26.AV-Qtn"
    next
end

config system dhcp server
    edit <id>
        set interface "AV-Qtn"
        config ip-range
            edit <id>
                set start-ip 10.111.0.2
                set end-ip 10.111.0.254
            next
        ...
    end

config user quarantine
    set quarantine {enable | disable}
end
```

To list stations in quarantine, use the following diagnose command:

```
diagnose wireless-controller wlac -c sta-qtn
```

## Host quarantine per SSID

Upon creating or editing an SSID, a **Quarantine Host** option is available to enable (by default) or disable quarantining devices that are connected in Tunnel-mode. The option to quarantine a device is available on **Topology** and **FortiView** WiFi pages.

When a host is put into quarantine VLAN, it will get its IP from the quarantine VLAN's DHCP server, and become part of the quarantined network.

### Syntax

```
config wireless-controller vap
    edit <name>
        set quarantine {enable | disable}
    next
end
```

To list all stations in quarantine:

```
diagnose wireless-controller wlac -c sta-qtn
```

## Locate a FortiAP with LED blinking

If you have an environment that contains numerous APs, and there is one AP that you need to frequently monitor, you can configure it to blink in the FortiCloud web portal. The blinking AP will be easier to locate.

**To start or stop LED blinking of a managed FortiAP, using the GUI:**

1. Go to **WiFi & Switch Controller > Managed FortiAPs**.
2. Right-click in the row of the device you want to control.

3. In the dialog box, scroll down to **LED Blink** and select **Start** or **Stop**.

The following models support LED blink control through the GUI, operating on FortiAP software 6.0.1, or later:

- FortiAP-112D, 221C, 223C, 224D, 320C, 321C
- FortiAP-S/W2

#### To start or stop LED blinking of a managed FortiAP, using the CLI:

```
execute wireless-controller led-blink <wtp-id> {on | on 10 | off}
```

The following models support LED blink control through the CLI, operating on FortiAP software 5.6.2, or later:

- FortiAP-112D, 221C, 223C, 224D, 320C, 321C
- FortiAP-S/W2

## Wireless controller optimization for large deployment - AP image upgrade

Using the CLI to upgrade FortiAP image is the preferred method especially for large deployments. Use the following execute command to upload the desired FortiAP image on the controller:

```
execute wireless-controller upload-wtp-image
```

After entering the command, reboot the FortiAP devices. This feature allows the administrator to configure all FortiAP devices to download the image from the controller at join time.

#### Syntax

```
config wireless-controller global
  set image-download {enable | disable}
end
```

To fine-tune this process, in order to deploy FortiAP image upgrades to a subset of devices for pilot testing, use the following command:

```
config wireless-controller wtp
  edit <name>
    set image-download {enable | disable}
  next
end
```

## Control message off-loading and aeroscout enhancement

Users can configure control message off-loading to optimize performance. This is especially useful in environments where the AP count is around 300-350 (with a device count between 1500 and 3000), where existing users are disconnected and unable to reauthenticate due to high CPU usage. This feature includes aeroscout enhancements.

#### Syntax

```
config wireless-controller global
  set control-message-offload {evp-frame | areoscout-tag | ap-list | sta-list | sta-cap-
    list | stats | aeroscout-mu}
```

```
end

config wireless-controller wtp-profile
  edit <name>
    set control-message-offload {enable | disable}
    config lbs
      set ekahau-blink-mode {enable | disable}
      set aeroscout {enable | disable}
      set aeroscout-server-ip <address>
      set aeroscout-server-port <UDP listening port>
      set aeroscout-mu {enable | disable}
    end
  end
end
```

# Protecting the WiFi network

Wireless IDS

WiFi data channel encryption

Protected Management Frames and Opportunistic Key Caching support

Preventing local bridge traffic from reaching the LAN

FortiAP-S bridge mode security profiles

DHCP snooping and option 82 (circuit-id) options for wireless access points

## Wireless IDS

The FortiGate Wireless Intrusion Detection System (WIDS) monitors wireless traffic for a wide range of security threats by detecting and reporting on possible intrusion attempts. When an attack is detected the FortiGate unit records a log message.

You can create a WIDS profile to enable these types of intrusion detection:

- Asleep Attack—ASLEAP is a tool used to perform attacks against LEAP authentication.
- Association Frame Flooding—A Denial of Service attack using a large number of association requests. The default detection threshold is 30 requests in 10 seconds.
- Authentication Frame Flooding—A Denial of Service attack using a large number of association requests. The default detection threshold is 30 requests in 10 seconds.
- Broadcasting De-authentication—This is a type of Denial of Service attack. A flood of spoofed de-authentication frames forces wireless clients to de-authenticate, then re-authenticate with their AP.
- EAPOL Packet Flooding—Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication. Flooding the AP with these packets can be a denial of service attack. Several types of EAPOL packets are detected: EAPOL-FAIL, EAPOL-LOGOFF, EAPOL-START, EAPOL-SUCC.
- Invalid MAC OUI—Some attackers use randomly-generated MAC addresses. The first three bytes of the MAC address are the Organizationally Unique Identifier (OUI), administered by IEEE. Invalid OUIs are logged.
- Long Duration Attack—To share radio bandwidth, WiFi devices reserve channels for brief periods of time. Excessively long reservation periods can be used as a denial of service attack. You can set a threshold between 1000 and 32 767 microseconds. The default is 8200.
- Null SSID Probe Response—When a wireless client sends out a probe request, the attacker sends a response with a null SSID. This causes many wireless cards and devices to stop responding.
- Spoofed De-authentication—Spoofed de-authentication frames are a denial of service attack. They cause all clients to disconnect from the AP.
- Weak WEP IV Detection—A primary means of cracking WEP keys is by capturing 802.11 frames over an extended period of time and searching for patterns of WEP initialization vectors (IVs) that are known to be weak. WIDS detects known weak WEP IVs in on-air traffic.
- Wireless Bridge—WiFi frames with both the fromDS and ToDS fields set indicate a wireless bridge. This will also detect a wireless bridge that you intentionally configured in your network.

You can enable wireless IDS by selecting a WIDS Profile in your FortiAP profile.

### To create a WIDS Profile

1. Go to **WiFi & Switch Controller > WIDS Profiles**.
2. Select a profile to edit or select **Create New**.
3. Select the types of intrusion to protect against.  
By default, all types are selected.
4. Select **Apply**.

You can also configure a WIDS profile in the CLI using the `config wireless-controller wids-profile` command.

## Rogue AP detection

The WIDS profile includes settings for detection of unauthorized (rogue) access points in your wireless network. For more information, see [Wireless network monitoring on page 114](#).

## WIDS client deauthentication rate for DoS attacks

As part of mitigating a Denial of Service (DoS) attack, the FortiGate sends deauthentication packets to unknown clients. In an aggressive attack, this deauthentication activity can prevent the processing of packets from valid clients. A WIDS Profile option in the CLI limits the deauthentication rate.

```
config wireless-controller wids-profile
  edit default
    set deauth-unknown-src-thresh <1-65535>
  end
```

The value set is a measure of the number of deauthorizations per second. 0 means no limit. The default is 10.

## WiFi data channel encryption

Optionally, you can apply DTLS encryption to the data channel between the wireless controller and FortiAP units. This enhances security.

There are data channel encryption settings on both the FortiGate unit and the FortiAP units. At both ends, you can enable Clear Text, DTLS encryption, or both. The settings must agree or the FortiAP unit will not be able to join the WiFi network. By default, both Clear Text and DTLS-encrypted communication are enabled on the FortiAP unit, allowing the FortiGate setting to determine whether data channel encryption is used. If the FortiGate unit also enables both Clear Text and DTLS, Clear Text is used.

Data channel encryption settings are located in the FortiAP profile. By default, only Clear Text is supported.



Data channel encryption is software-based and can affect performance. Verify that the system meets your performance requirements with encryption enabled.

## Configuring encryption on the FortiGate unit

You can use the CLI to configure data channel encryption.

## Enabling encryption

In the CLI, the `wireless wtp-profile` command contains a new field, `dtls-policy`, with options `clear-text` and `dtls-enabled`. To enable encryption in profile1 for example, enter:

```
config wireless-controller wtp-profile
  edit profile1
    set dtls-policy dtls-enabled
  end
```

## Configuring encryption on the FortiAP unit

The FortiAP unit has its own settings for data channel encryption.

### Enabling CAPWAP encryption - FortiAP web-based manager

1. On the **System Information** page, in **WTP Configuration > AC Data Channel Security**, select one of:
  - Clear Text
  - DTLS Enabled
  - Clear Text or DTLS Enabled (default)
2. Select **Apply**.

### Enabling encryption - FortiAP CLI

You can set the data channel encryption using the `AP_DATA_CHAN_SEC` variable: 'clear', or 'ipsec', or 'dtls'.

For example, to set security to DTLS and then save the setting, enter:

```
cfg -a AP_DATA_CHAN_SEC=dtls
cfg -c
```

## Protected Management Frames and Opportunistic Key Caching support

Protected Management Frames (PMF) protect some types of management frames like deauthorization, disassociation and action frames. This feature, now mandatory on WiFi certified 802.11ac devices, prevents attackers from sending plain deauthorization/disassociation frames to disrupt or tear down a connection/association. PMF is a Wi-Fi Alliance specification based on IEEE 802.11w.

To facilitate faster roaming client roaming, you can enable Opportunistic Key Caching (OKC) on your WiFi network. When a client associates with an AP, its PMK identifier is sent to all other APs on the network. This eliminates the need for an already-authenticated client to repeat the full EAP exchange process when it roams to another AP on the same network.

Use of PMF and OKC on an SSID is configurable only in the CLI:

```
config wireless-controller vap
  edit <vap_name>
    set pmf {disable | enable | optional}
    set pmf-assoc-comeback-timeout <integer>
    set pmf-sa-query-retry-timeout <integer>
    set okc {disable | enable}
  next
end
```

When `pmf` is set to `optional`, it is considered enabled, but will allow clients that do not use PMF. When `pmf` is set to `enable`, PMF is required by all clients.

## Bluetooth Low Energy (BLE) Scan

The FortiGate can configure FortiAP Bluetooth Low Energy (BLE) scan, incorporating Google's BLE beacon profile known as Eddystone, used to identify groups of devices and individual devices.



Currently, only the FAP-S221E, FAP-S223E, and FAP-222E models support this feature.

Use the following syntax to configure BLE profiles, configure BLE report intervals, and assign BLE profiles to WTP profiles.

### CLI syntax - Configure BLE profiles

```
config wireless-controller ble-profile
  edit <name>
    set comment <comment>
    set advertising {ibeacon | eddystone-uid | eddystone-url}
    set ibeacon-uuid <uuid>
    set major-id <0 - 65535> - (default = 1000)
    set minor-id <0 - 65535> - (default = 1000)
    set eddystone-namespace <10-byte namespace>
    set eddystone-instance <device id>
    set eddystone-url <url>
    set txpower <0 - 12> - (default = 0)
    set beacon-interval <40 - 3500> - (default = 100)
    set ble-scanning {enable | disable} - (default = disable)
  next
end
```

Note that `txpower` determines the transmit power level on a scale of 0-12:

<b>0:</b> -21 dBm	<b>1:</b> -18 dBm	<b>2:</b> -15 dBm	<b>3:</b> -12 dBm	<b>4:</b> -9 dBm
<b>5:</b> -6 dBm	<b>6:</b> -3 dBm	<b>7:</b> 0 dBm	<b>8:</b> 1 dBm	<b>9:</b> 2 dBm
<b>10:</b> 3 dBm	<b>11:</b> 4 dBm	<b>12:</b> 5 dBm		

### CLI syntax - Configure BLE report intervals

```
config wireless-controller timers
  set ble-scan-report-intv - (default = 30 sec)
end
```

### CLI syntax - Assign BLE profiles to WTP profiles

```
config wireless-controller wtp-profile
  edit <name>
    set ble-profile <name>
  next
```

```
end
```

## Preventing local bridge traffic from reaching the LAN

The following command can be enabled so that when a client connects to a VAP, and its traffic is not tunneled to the controller, the admin can control whether the client can access the local network.

Note that this entry is only available when `local-standalone-nat` is set to `enable`.

### Syntax:

```
config wireless-controller vap
  edit <name>
    set local-lan {allow | deny}
  next
end
```

## FortiAP-S bridge mode security profiles

If you have enabled bridge mode for a managed FortiAP-S, you can add a UTM profile to the wireless controller configuration that allows you to apply the following security profile features to all traffic accepted by the managed FortiAP-S:

- AntiVirus (including Botnet protection),
- IPS,
- Application control, and
- Web Filtering.

You can use the following CLI command to add a wireless controller UTM profile:

```
config wireless-controller utm-profile
  edit <name>
    set comment "Default configuration for offloading WiFi traffic."
    set ips-sensor "wifi-default"
    set application-list "wifi-default"
    set antivirus-profile "wifi-default"
    set webfilter-profile "wifi-default"
    set firewall-profile-protocol-options "wifi-default"
    set firewall-ssl-ssh-profile "wifi-default"
  next
end
```

You can use the following CLI command to add a wireless controller UTM profile to a wireless SSID (virtual access point) configuration:

```
config wireless-controller vap
  edit <name>
    set utm-profile
  end
end
```



## DHCP snooping and option 82 (circuit -id) options for wireless access points

New commands are available to enable or disable (by default) DHCP 82 option insertion for wireless access points. DHCP snooping is used to prevent rogue DHCP servers from offering IP addresses to DHCP clients.

### Syntax

```
config wireless-controller vap
  edit wifi
    set dhcp-option82-insertion {enable | disable}
    set dhcp-option82-circuit-id-insertion {style-1 | style-2 | disable}
    set dhcp-option82-remote-id-insertion {style-1 | disable}
  next
end
```

# Wireless network monitoring

You can monitor both your wireless clients and other wireless networks that are available in your coverage area.

[Monitoring wireless clients](#)

[Monitoring rogue APs](#)

[Suppressing rogue APs](#)

[Monitoring wireless network health](#)

## Monitoring wireless clients

**To view connected clients on a FortiWiFi unit**

1. Go to **Monitor > Client Monitor**.

The following information is displayed:

<b>SSID</b>	The SSID that the client connected to.
<b>FortiAP</b>	The serial number of the FortiAP unit to which the client connected.
<b>User</b>	User name
<b>IP</b>	The IP address assigned to the wireless client.
<b>Device</b>	
<b>Auth</b>	The type of authentication used.
<b>Channel</b>	WiFi radio channel in use.
<b>Bandwidth Tx/Rx</b>	Client received and transmitted bandwidth, in Kbps.
<b>Signal Strength / Noise</b>	The signal-to-noise ratio in decibels calculated from signal strength and noise level.
<b>Signal Strength</b>	
<b>Association Time</b>	How long the client has been connected to this access point.

Results can be filtered. Select the filter icon on the column you want to filter. Enter the values to include or select NOT if you want to exclude the specified values.

## Monitoring rogue APs

The access point radio equipment can scan for other available access points, either as a dedicated monitor or in idle periods during AP operation.

Discovered access points are listed in **Monitor > Rogue AP Monitor**. You can then mark them as either Accepted or Rogue access points. This designation helps you to track access points. It does not affect anyone's ability to use these access points.

It is also possible to suppress rogue APs. See [Monitoring rogue APs on page 114](#).

## On-wire rogue AP detection technique

Other APs that are available in the same area as your own APs are not necessarily rogues. A neighboring AP that has no connection to your network might cause interference, but it is not a security threat. A rogue AP is an unauthorized AP connected to your wired network. This can enable unauthorized access. When rogue AP detection is enabled, the **On-wire** column in the **Rogue AP Monitor** list shows a green up-arrow on detected rogues.

Rogue AP monitoring of WiFi client traffic builds a table of WiFi clients and the Access Points that they are communicating through. The FortiGate unit also builds a table of MAC addresses that it sees on the LAN. The FortiGate unit's on-wire correlation engine constantly compares the MAC addresses seen on the LAN to the MAC addresses seen on the WiFi network.

There are two methods of Rogue AP on-wire detection operating simultaneously: Exact MAC address match and MAC adjacency.

### Exact MAC address match

If the same MAC address is seen on the LAN and on the WiFi network, this means that the wireless client is connected to the LAN. If the AP that the client is using is not authorized in the FortiGate unit configuration, that AP is deemed an 'on-wire' rogue. This scheme works for non-NAT rogue APs.

### MAC adjacency

If an access point is also a router, it applies NAT to WiFi packets. This can make rogue detection more difficult. However, an AP's WiFi interface MAC address is usually in the same range as its wired MAC address. So, the MAC adjacency rogue detection method matches LAN and WiFi network MAC addresses that are within a defined numerical distance of each other. By default, the MAC adjacency value is 7. If the AP for these matching MAC addresses is not authorized in the FortiGate unit configuration, that AP is deemed an 'on-wire' rogue.

### Limitations

On-wire rogue detection has some limitations. There must be at least one WiFi client connected to the suspect AP and continuously sending traffic. If the suspect AP is a router, its WiFi MAC address must be very similar to its Ethernet port MAC address.

### Logging

Information about detected rogue APs is logged and uploaded to your FortiAnalyzer unit, if you have one. By default, rogue APs generate an alert level log, unknown APs generate a warning level log. This log information can help you with PCI-DSS compliance requirements.

## Rogue AP scanning as a background activity

Each WiFi radio can perform monitoring of radio channels in its operating band while acting as an AP. It does this by briefly switching from AP to monitoring mode. By default, a scan period starts every 300 seconds. Each second a different channel is monitored for 20ms until all channels have been checked.

During heavy AP traffic, it is possible for Spectrum Analysis background scanning to cause lost packets when the radio switches to monitoring. To reduce the probability of lost packets, you can set the CLI `ap-bgscan-idle` field to delay the switch to monitoring until the AP has been idle for a specified period. This means that heavy AP traffic may slow background scanning.

The following CLI example configures default background rogue scanning operation except that it sets `ap-bgscan-idle` to require 100ms of AP inactivity before scanning the next channel.

```
config wireless-controller wtp-profile
  edit ourprofile
    config radio-1
      set wids-profile ourwidsprofile
      set spectrum-analysis enable
    end
  end
config wireless-controller wids-profile
  edit ourwidsprofile
    set ap-scan enable
    set rogue-scan enable
    set ap-bgscan-period 300
    set ap-bgscan-intv 1
    set ap-bgscan-duration 20
    set ap-bgscan-idle 100
  end
```

## Configuring rogue scanning

All APs using the same FortiAP Profile share the same rogue scanning settings, unless override is configured.

### To enable rogue AP scanning with on-wire detection - web-based manager

1. Go to **WiFi & Switch Controller > WIDS Profiles**.  
On some models, the menu is **WiFi & Switch Controller**.
2. Select an existing WIDS Profile and edit it, or select **Create New**.
3. Make sure that **Enable Rogue AP Detection** is selected.
4. Select **Enable On-Wire Rogue AP Detection**.
5. Optionally, enable **Auto Suppress Rogue APs in Foreground Scan**.
6. Select **OK**.

### To enable the rogue AP scanning feature in a custom AP profile - CLI

```
config wireless-controller wids-profile
  edit FAP220B-default
    set ap-scan enable
    set rogue-scan enable
  end
```

## Exempting an AP from rogue scanning

By default, if Rogue AP Detection is enabled, it is enabled on all managed FortiAP units. Optionally, you can exempt an AP from scanning. You should be careful about doing this if your organization must perform scanning to meet PCI-DSS requirements.

**To exempt an AP from rogue scanning**

1. Go to **WiFi & Switch Controller > WIDS Profiles**.
2. Create a new WIDS profile and disable **Rogue AP detection**.
3. Go to **WiFi & Switch Controller > FortiAP Profiles** and edit the profile you wish to exempt from rogue scanning.
4. Assign the WIDS profile created in step 2.

**MAC adjacency**

You can adjust the maximum WiFi to Ethernet MAC difference used when determining whether an suspect AP is a rogue.

**To adjust MAC adjacency**

For example, to change the adjacency to 8, enter








```
config wireless-controller global
  set rogue-scan-mac-adjacency 8
end
```

## Using the Rogue AP Monitor

Go to **Monitor > Rogue AP Monitor** to view the list of other wireless access points that are receivable at your location.

### Information Columns

Actual columns displayed depends on **Column Settings**.

<b>State</b>	 Rogue AP — Use this status for unauthorized APs that <b>On-wire</b> status indicates are attached to your wired networks.
	 Accepted AP — Use this status for APs that are an authorized part of your network or are neighboring APs that are not a security threat. To see accepted APs in the list, select <b>Show Accepted</b> .
	 Unclassified — This is the initial status of a discovered AP. You can change an AP back to unclassified if you have mistakenly marked it as Rogue or Accepted.
<b>Online Status</b>	 Active AP
	 Inactive AP
	 Active ad-hoc WiFi device
	 Inactive ad-hoc WiFi device
<b>SSID</b>	The wireless service set identifier (SSID) or network name for the wireless interface.
<b>Security Type</b>	The type of security currently being used.
<b>Channel</b>	The wireless radio channel that the access point uses.
<b>MAC Address</b>	The MAC address of the Wireless interface.
<b>Vendor Info</b>	The name of the vendor.
<b>Signal Strength</b>	The relative signal strength of the AP. Mouse over the symbol to view the signal-to-noise ratio.
<b>Detected By</b>	The name or serial number of the AP unit that detected the signal.
<b>On-wire</b>	A green up-arrow indicates a suspected rogue, based on the on-wire detection technique. A red down-arrow indicates AP is not a suspected rogue.
<b>First Seen</b>	How long ago this AP was first detected.

<b>Last Seen</b>	How long ago this AP was last detected.
<b>Rate</b>	Data rate in bps.

To change the Online Status of an AP, right-click it and select Mark Accepted or Mark Rogue.

## Suppressing rogue APs

In addition to monitoring rogue APs, you can actively prevent your users from connecting to them. When suppression is activated against an AP, the FortiGate WiFi controller sends deauthentication messages to the rogue AP's clients, posing as the rogue AP, and also sends deauthentication messages to the rogue AP, posing as its clients. This is done using the monitoring radio.



Before enabling this feature, verify that operation of Rogue Suppression is compliant with the applicable laws and regulations of your region.

To enable rogue AP suppression, you must enable monitoring of rogue APs with the on-wire detection technique. See ["Monitoring rogue APs"](#). The monitoring radio must be in the Dedicated Monitor mode.

### To activate AP suppression against a rogue AP

1. Go to **Monitor > Rogue AP Monitor**.
2. When you see an AP listed that is a rogue detected "on-wire", select it and then select **Mark > Mark Rogue**.
3. To suppress an AP that is marked as a rogue, select it and then select **Suppress AP**.

### To deactivate AP suppression

1. Go to **Monitor > Rogue AP Monitor**.
2. Select the suppressed rogue AP and then select **Suppress AP > Unsuppress AP**.

## Monitoring wireless network health

To view the wireless health dashboard, go to **Monitor > WiFi Health Monitor**.

The wireless health dashboard provides a comprehensive view of the health of your network's wireless infrastructure. The dashboard includes widgets to display:

- **AP Status**

Active, Down or missing, up for over 24 hours, rebooted in past 24 hours

- **Client Count Over Time**

Viewable for past hour, day, or 30 days

- **Top Client Count Per-AP**

Separate widgets for 2.4GHz and 5GHz bands

- **Top Wireless Interference**

Separate widgets for 2.4GHz and 5GHz bands, requires spectrum analysis to be enabled on the radios

- **Login Failures Information**

- **WiFi Channel Utilization**

Three views allowing users to view top 10-20 Most and Least utilized channels for each AP radio and a third histogram view showing counts for utilization

The list of active clients also shows MAC address entries (similar to the **WiFi Client Monitor** page), making client information easy to view when opening the **Active Client** widget.



# Configuring wireless network clients

This chapter shows how to configure typical wireless network clients to connect to a wireless network with WPA-Enterprise security.

Windows XP client

Windows 7 client

Mac OS client

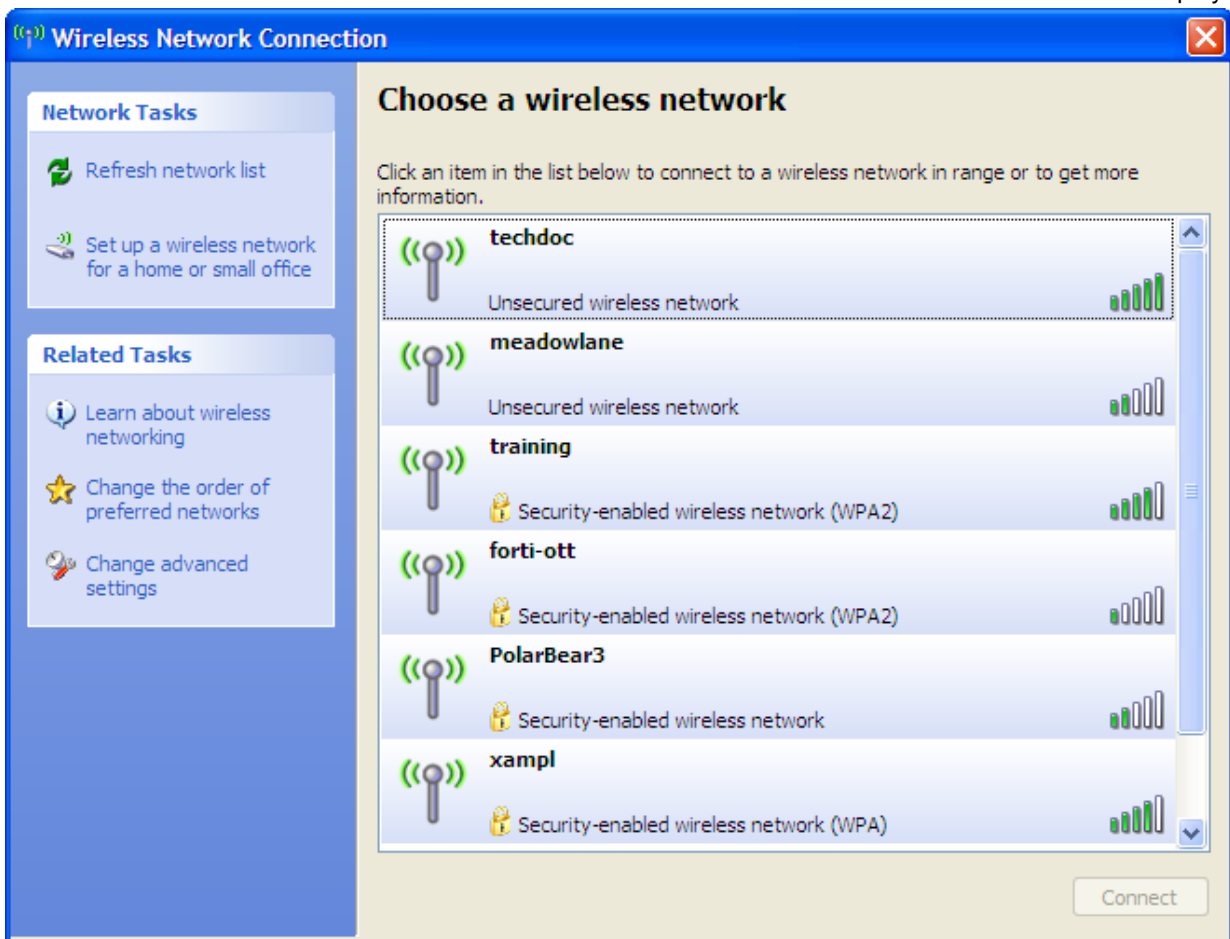
Linux client

Troubleshooting

## Windows XP client

**To configure the WPA-Enterprise network connection**

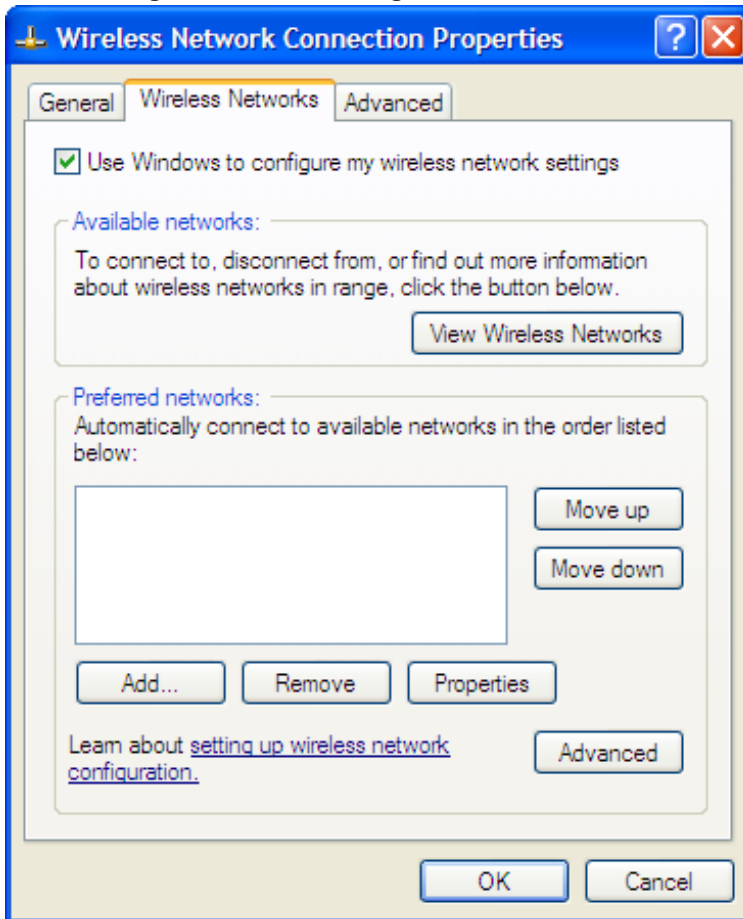
1. In the Windows Start menu, go to **Control Panel > Network Connections > Wireless Network Connection** or select the wireless network icon in the Notification area of the Taskbar. A list of available networks is displayed.



If you are already connected to another wireless network, the Connection Status window displays. Select **View Wireless Networks** on the **General** tab to view the list.

If the network broadcasts its SSID, it is listed. But do not try to connect until you have completed the configuration step below. Because the network doesn't use the Windows XP default security configuration, configure the client's network settings manually before trying to connect.

2. You can configure the WPA-Enterprise network to be accessible from the **View Wireless Networks** window even if it does not broadcast its SSID.
3. Select **Change Advanced Settings** and then select the **Wireless Networks** tab.



Any existing networks that you have already configured are listed in the **Preferred Networks** list.

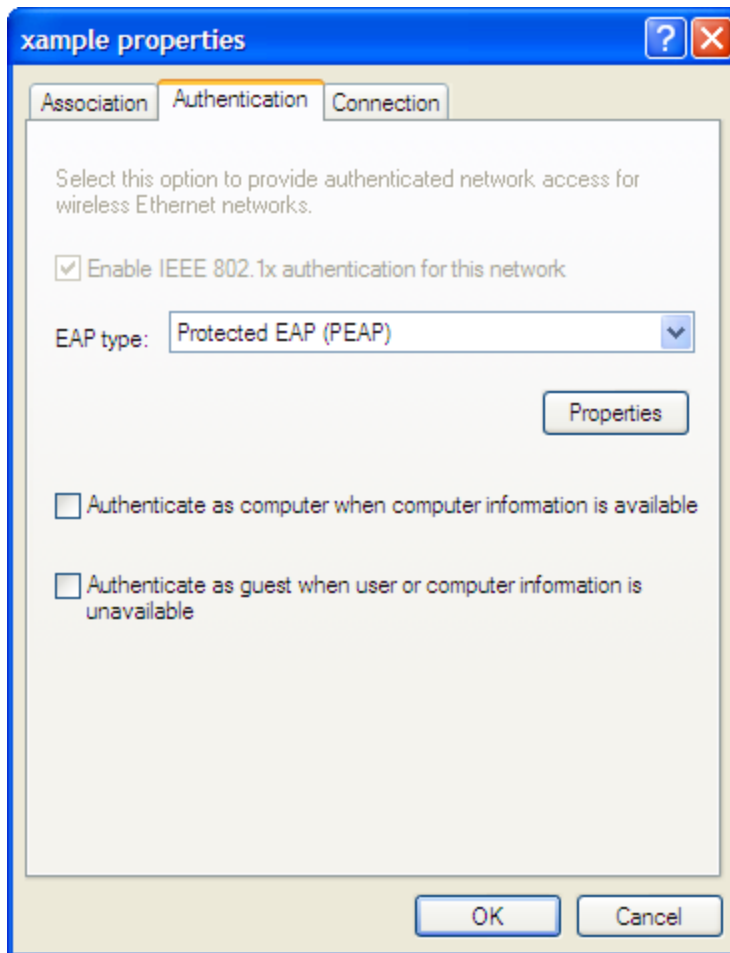
4. Select **Add** and enter the following information:

The screenshot shows the 'Wireless network properties' dialog box with the 'Authentication' tab selected. The 'Association' tab is also visible. The 'Network name (SSID)' field contains 'xample'. The 'Connect even if this network is not broadcasting' checkbox is unchecked. The 'Wireless network key' section is expanded, showing 'This network requires a key for the following:'. The 'Network Authentication' dropdown is set to 'WPA2' and the 'Data encryption' dropdown is set to 'AES'. The 'Network key' and 'Confirm network key' fields are empty. The 'Key index (advanced)' spinner is set to '1'. The 'The key is provided for me automatically' checkbox is unchecked. The 'This is a computer-to-computer (ad hoc) network; wireless access points are not used' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom.

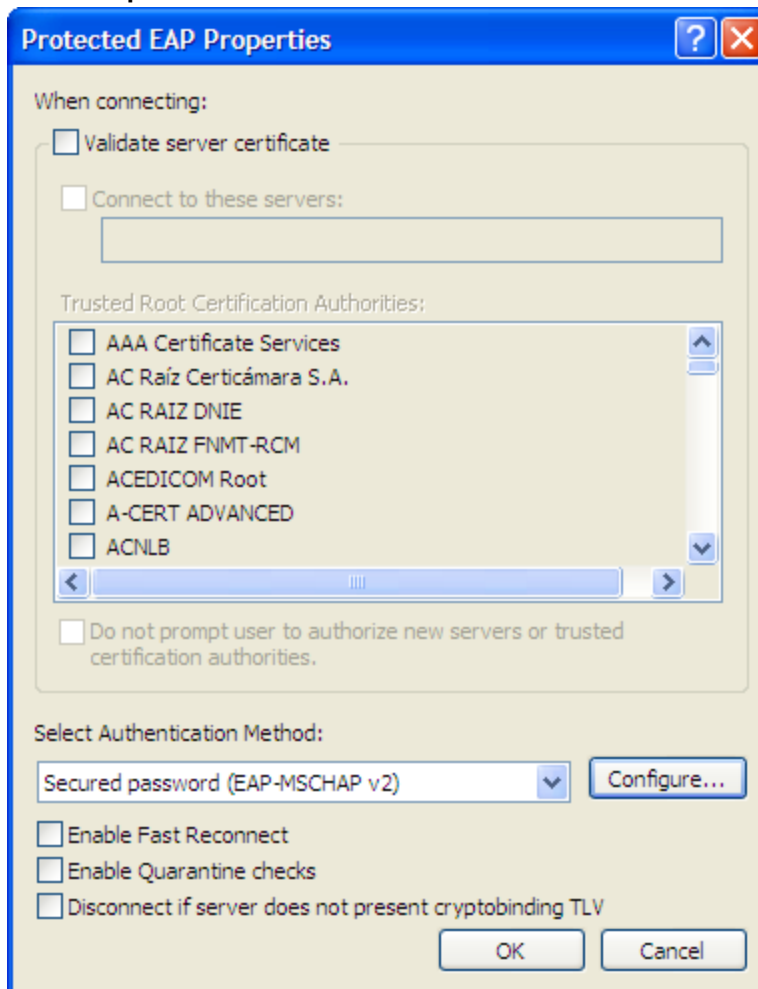
<b>Network Name (SSID)</b>	The SSID for your wireless network
<b>Network Authentication</b>	WPA2
<b>Data Encryption</b>	AES

5. If this wireless network does not broadcast its SSID, select **Connect even if this network is not broadcasting** so that the network will appear in the **View Wireless Networks** list.

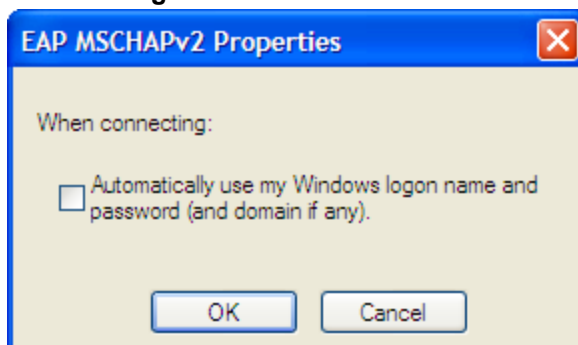
6. Select the **Authentication** tab.



7. In **EAP Type**, select **Protected EAP (PEAP)**.
8. Make sure that the other two authentication options are not selected.

9. Select **Properties**.

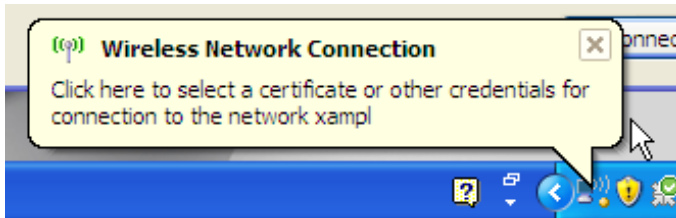
10. Make sure that **Validate server certificate** is selected.
11. Select the server certificate **Entrust Root Certification Authority**.
12. In **Select Authentication Method**, select **Secured Password (EAP-MSCHAPv2)**.
13. Ensure that the remaining options are not selected.
14. Select **Configure**.



15. If your wireless network credentials are the same as your Windows logon credentials, select **Automatically use my Windows logon name and password**. Otherwise, make sure that this option is not selected.
16. Select **OK**. Repeat until you have closed all of the **Wireless Network Connection Properties** windows.

**To connect to the WPA-Enterprise wireless network**

1. Select the wireless network icon in the Notification area of the Taskbar.
2. In the **View Wireless Networks** list, select the network you just added and then select **Connect**. You might need to log off of your current wireless network and refresh the list.
3. When the following popup displays, click on it.



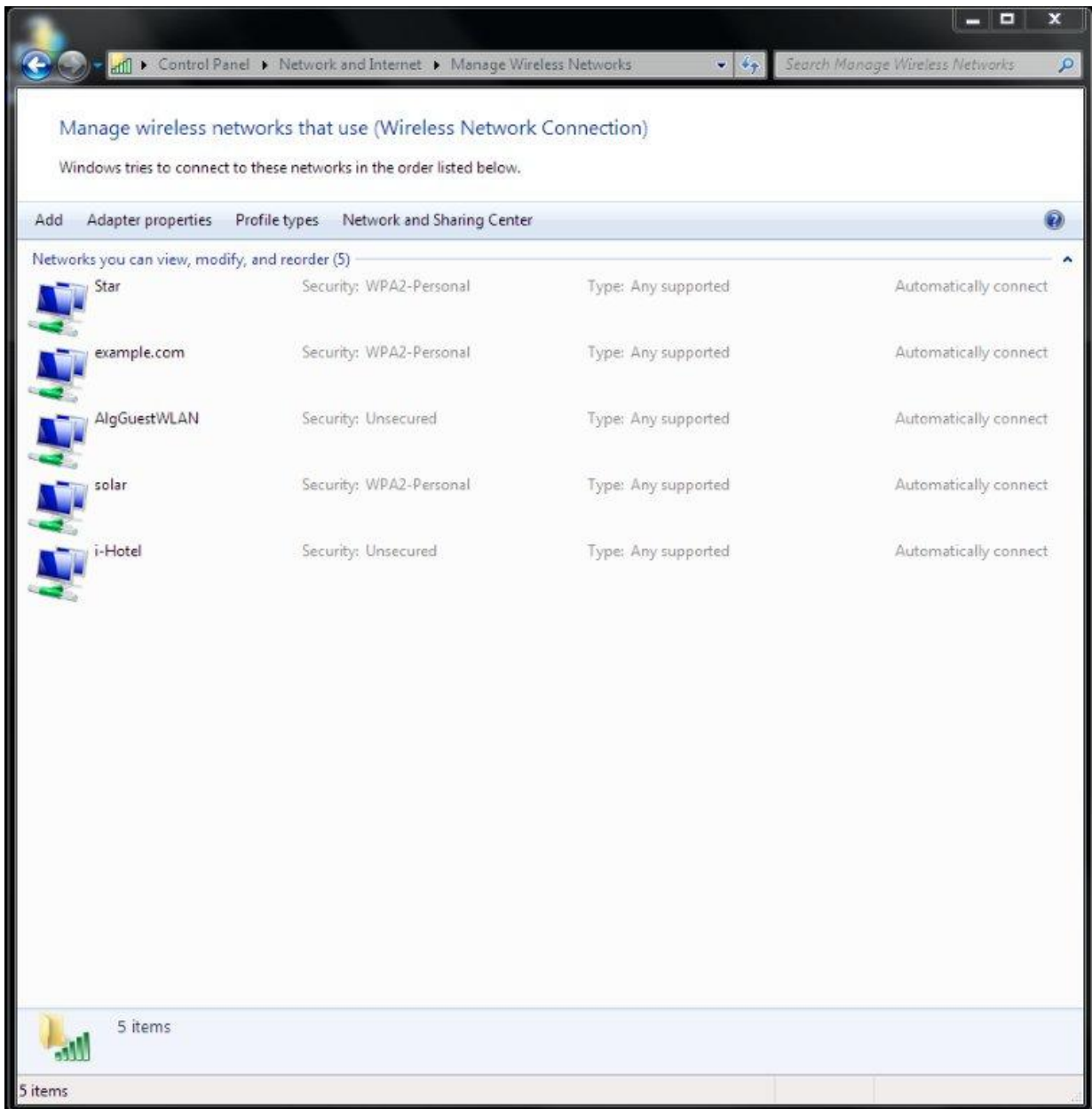
4. In the **Enter Credentials** window, enter your wireless network **User name**, **Password**, and **Logon domain** (if applicable). Then, select **OK**.



In future, Windows will automatically send your credentials when you log on to this network.

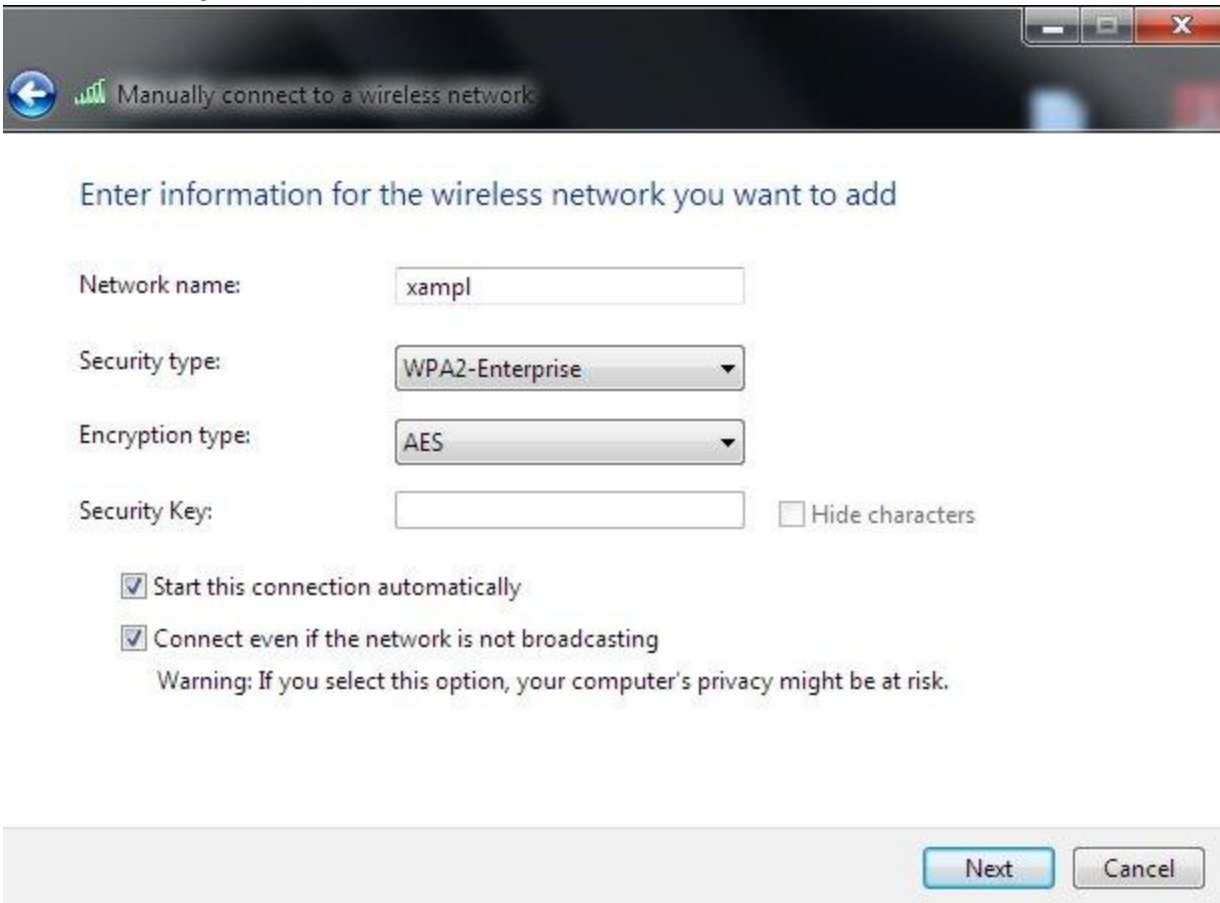
## Windows 7 client

1. In the Windows Start menu, go to **Control Panel > Network and Internet > Network and Sharing Center > Manage Wireless Networks** or select the wireless network icon in the Notification area of the Taskbar. A list of available networks is displayed.



2. Do one of the following:
  - If the wireless network is listed (it broadcasts its SSID), select it from the list.
  - Select **Add > Manually create a network profile**.

3. Enter the following information and select **Next**.



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:

Security type:

Encryption type:

Security Key:  ☐ Hide characters

☒ Start this connection automatically

☒ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

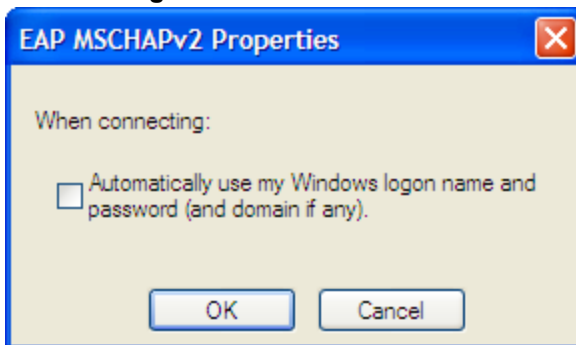
<b>Network name</b>	Enter the SSID of the wireless network. (Required only if you selected <b>Add</b> .)
<b>Security type</b>	WPA2-Enterprise
<b>Encryption type</b>	AES
<b>Start this connection automatically</b>	Select
<b>Connect even if the network is not broadcasting.</b>	Select

The Wireless Network icon will display a popup requesting that you click to enter credentials for the network. Click on the popup notification.

4. In the **Enter Credentials** window, enter your wireless network **User name**, **Password**, and **Logon domain** (if applicable). Then, select **OK**.
5. Select **Change connection settings**.
6. On the **Connection** tab, select **Connect automatically when this network is in range**.
7. On the **Security** tab, select the Microsoft PEAP authentication method and then select **Settings**.



8. Make sure that **Validate server certificate** is selected.
9. Select the server certificate **Entrust Root Certification Authority**.
10. In **Select Authentication Method**, select **Secured Password (EAP-MSCHAPv2)**.
11. Select **Configure**.

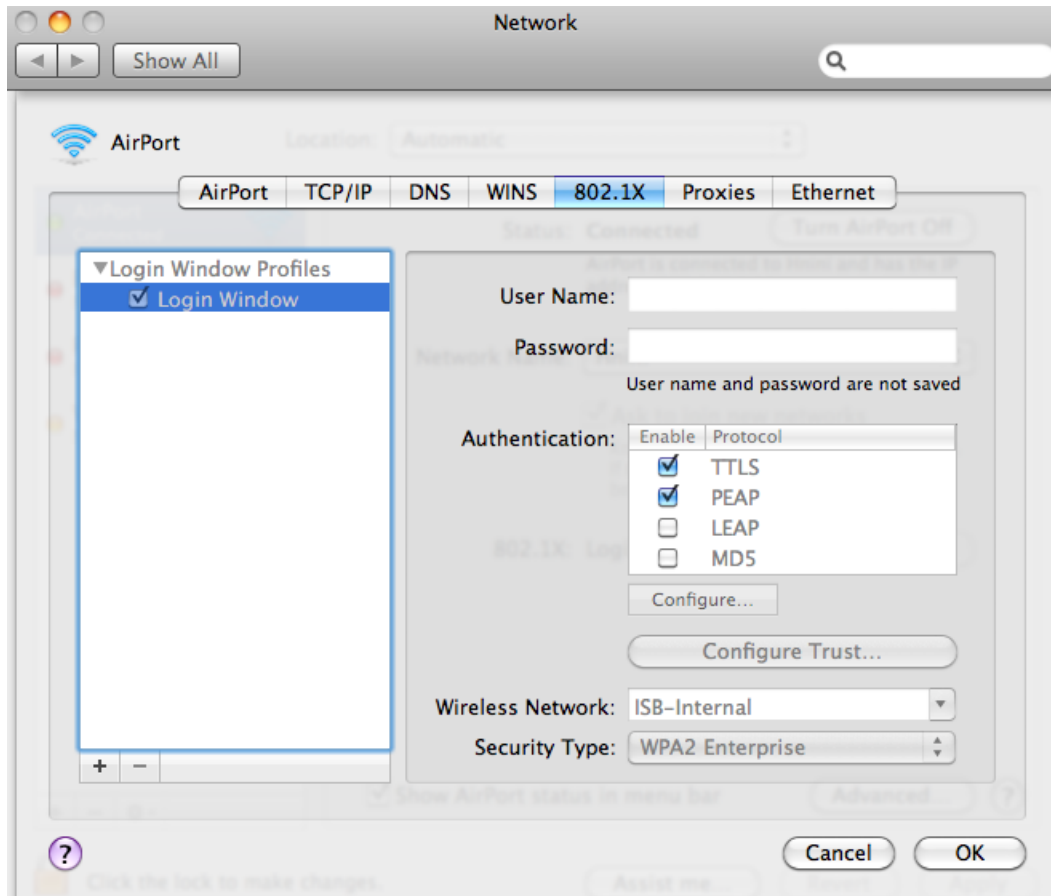


12. If your wireless network credentials are the same as your Windows logon credentials, select **Automatically use my Windows logon name and password**. Otherwise, make sure that this option is not selected.
13. Ensure that the remaining options are not selected.
14. Select **OK**. Repeat until you have closed all of the **Wireless Network Properties** windows.

## Mac OS client

### To configure network preferences

1. Right-click the **AirPort** icon in the toolbar and select **Open Network Preferences**.
2. Select **Advanced** and then select the **802.1X** tab.

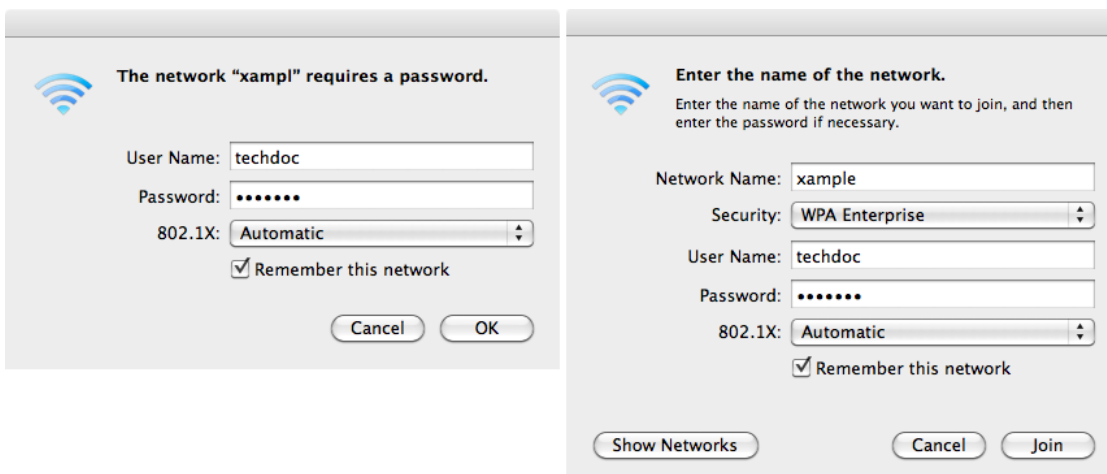


3. If there are no Login Window Profiles in the left column, select the + button and then select **Add Login Window Profile**.
4. Select the Login Window Profile and then make sure that both TTLS and PEAP are selected in **Authentication**.

### To configure the WPA-Enterprise network connection

1. Select the **AirPort** icon in the toolbar.
2. Do one of the following:
  - If the network is listed, select the network from the list.
  - Select **Connect to Other Network**.

One of the following windows opens, depending on your selection.



3. Enter the following information and select **OK** or **Join**:

<b>Network name</b>	Enter the SSID of your wireless network. (Other network only)
<b>Wireless Security</b>	WPA Enterprise
<b>802.1X</b>	Automatic
<b>Username Password</b>	Enter your logon credentials for the wireless network.
<b>Remember this network</b>	Select.

You are connected to the wireless network.



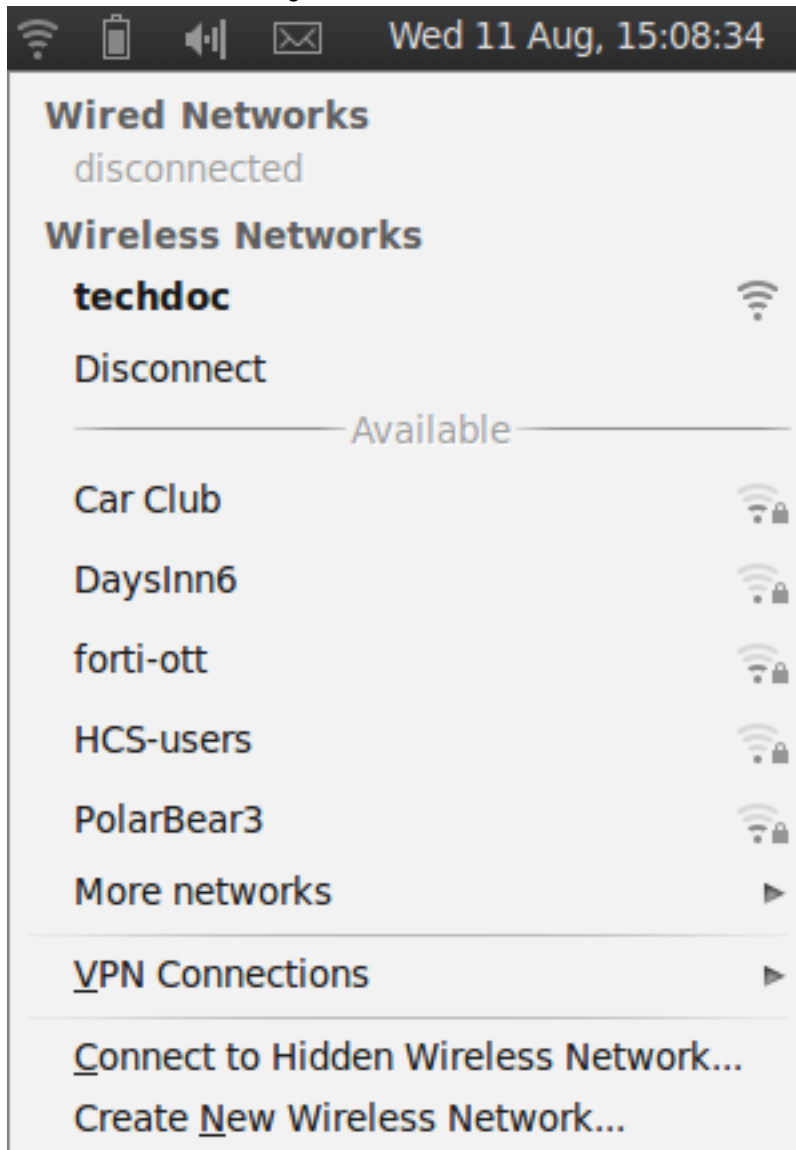
Mac OS supports only PEAP with MSCHAPv2 authentication and therefore can authenticate only to a RADIUS server, not an LDAP or TACACS+ server

## Linux client

This example is based on the Ubuntu 10.04 Linux wireless client.

### To connect to a WPA-Enterprise network

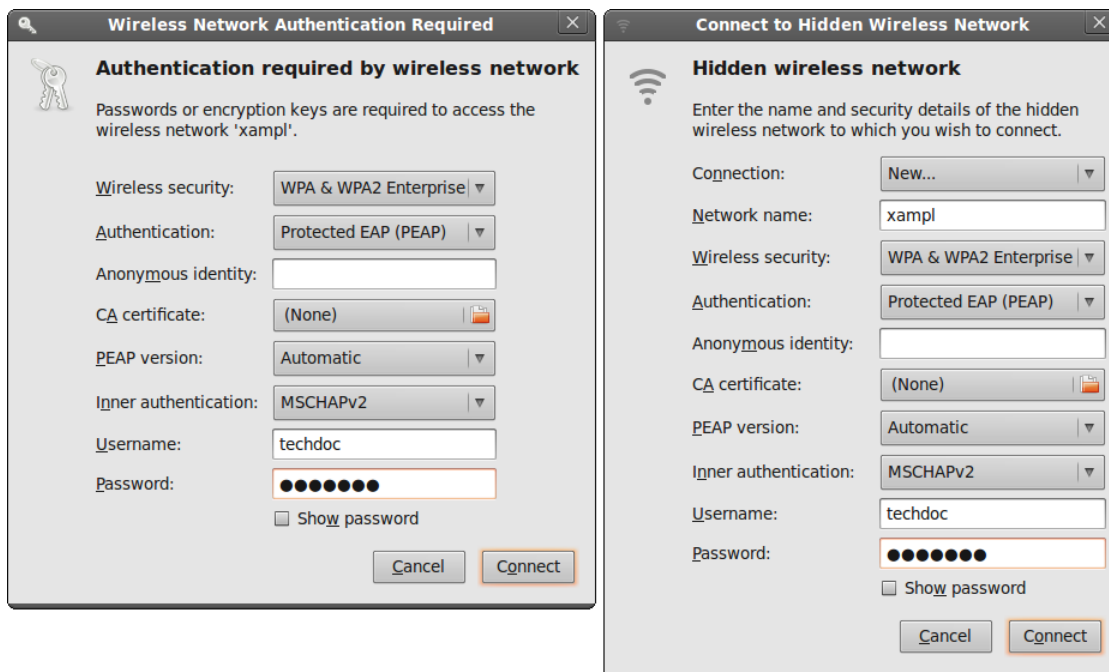
1. Select the Network Manager icon to view the Wireless Networks menu.



Wireless networks that broadcast their SSID are listed in the **Available** section of the menu. If the list is long, it is continued in the **More Networks** submenu.

2. Do one of the following:
  - Select the network from the list (also check **More Networks**).
  - Select **Connect to Hidden Wireless Network**.

One of the following windows opens, depending on your selection.



3. Enter the following information:

<b>Connection</b>	Leave as <b>New</b> . (Hidden network only)
<b>Network name</b>	Enter the SSID of your wireless network. (Hidden network only)
<b>Wireless Security</b>	WPA & WPA2 Enterprise
<b>Authentication</b>	Protected EAP (PEAP) for RADIUS-based authentication Tunneled TLS for TACACS+ or LDAP-based authentication
<b>Anonymous identity</b>	This is not required.
<b>CA Certificate</b>	If you want to validate the AP's certificate, select the <b>Entrust Root Certification Authority</b> root certificate. The default location for the certificate is /usr/share/ca-certificates/mozilla/.
<b>PEAP version</b>	Automatic (applies only to PEAP)
<b>Inner authentication</b>	MSCHAPv2 for RADIUS-based authentication PAP or CHAP for TACACS+ or LDAP-based authentication
<b>Username</b>	Enter your logon credentials for the wireless network.
<b>Password</b>	

4. If you did not select a CA Certificate above, you are asked to do so. Select Ignore.



5. Select **Connect**. You are connected to the wireless network.

#### To connect to a WPA-Enterprise network

1. Select the Network Manager icon to view the Wireless Networks menu.
2. Select the network from the list (also check **More Networks**).  
If your network is not listed (but was configured), select **Connect to Hidden Wireless Network**, select your network from the Connection drop-down list, and then select **Connect**.

## Troubleshooting

Using tools provided in your operating system, you can find the source of common wireless networking problems.

### Checking that client received IP address and DNS server information

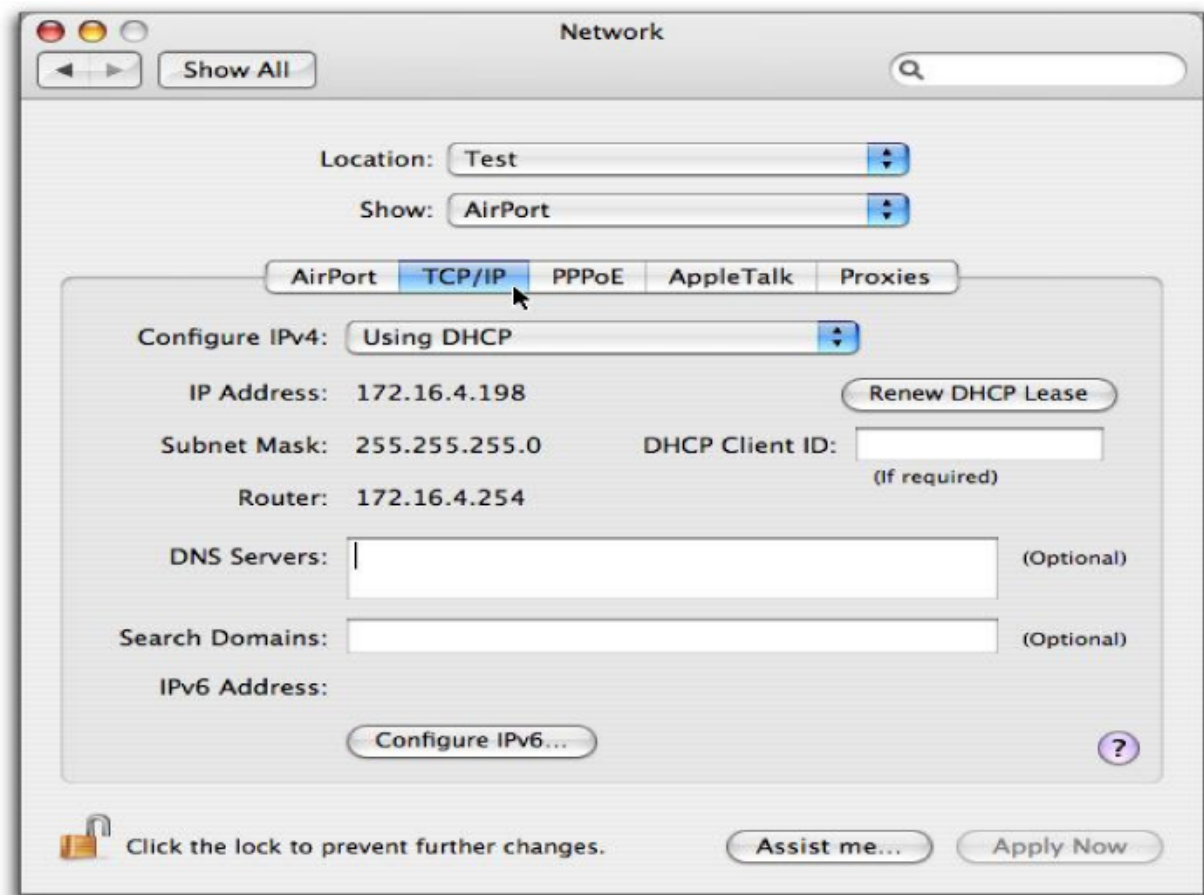
#### Windows XP

1. Double-click the network icon in the taskbar to display the **Wireless Network Connection Status** window. Check that the correct network is listed in the **Connection** section.
2. Select the **Support** tab.  
Check that the **Address Type** is **Assigned by DHCP**. Check that the **IP Address**, **Subnet Mask**, and **Default Gateway** values are valid.
3. Select **Details** to view the DNS server addresses.  
The listed address should be the DNS serves that were assigned to the WAP. Usually a wireless network that provides access to the private LAN is assigned the same DNS servers as the wired private LAN. A wireless network that provides guest or customer users access to the Internet is usually assigned public DNS servers.
4. If any of the addresses are missing, select **Repair**.  
If the repair procedure doesn't correct the problem, check your network settings.

#### Mac OS

1. From the Apple menu, open **System Preferences > Network**.
2. Select **AirPort** and then select **Configure**.

3. On the **Network** page, select the **TCP/IP** tab.



4. If there is no IP address or the IP address starts with 169, select **Renew DHCP Lease**.
5. To check DNS server addresses, open a terminal window and enter the following command:  

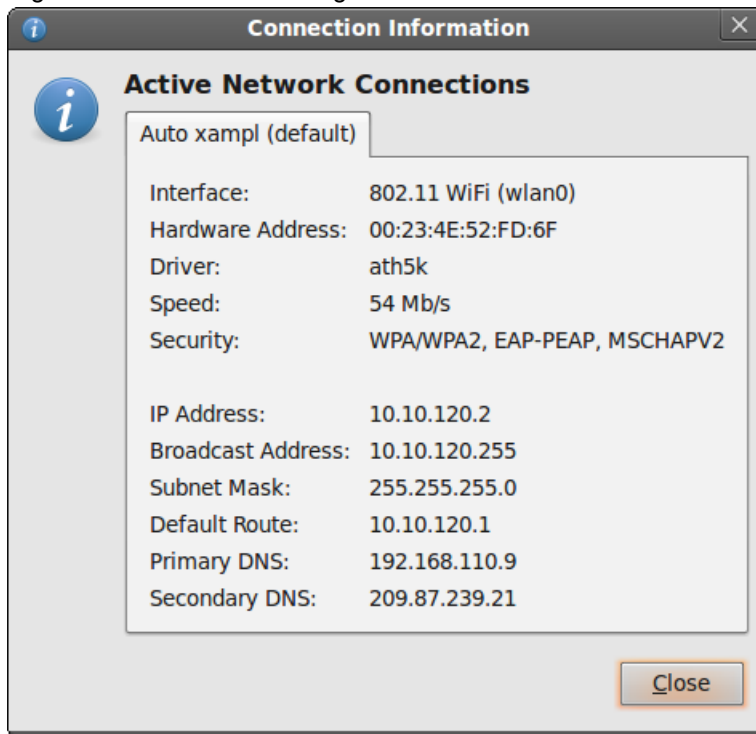
```
cat /etc/resolv.conf
```

Check the listed nameserver addresses. A network for employees should use the wired private LAN DNS server. A network for guests should specify a public DNS server.

## Linux

This example is based on the Ubuntu 10.04 Linux wireless client.

1. Right-click the Network Manager icon and select **Connection Information**.



2. Check the IP address, and DNS settings. If they are incorrect, check your network settings.



# Wireless network examples

This chapter provides an example wireless network configuration.

[Basic wireless network](#)

[A more complex example](#)

## Basic wireless network

This example uses automatic configuration to set up a basic wireless network.

To configure this wireless network, you must:

- Configure authentication for wireless users
- Configure the SSID (WiFi network interface)
- Add the SSID to the FortiAP Profile
- Configure the firewall policy
- Configure and connect FortiAP units

## Configuring authentication for wireless users

You need to configure user accounts and add the users to a user group. This example shows only one account, but multiple accounts can be added as user group members.

### To configure a WiFi user - web-based manager

1. Go to **User & Device > User Definition** and select **Create New**.
2. Select **Local User** and then click **Next**.
3. Enter a **User Name** and **Password** and then click **Next**.
4. Click **Next**.
5. Make sure that **Enable** is selected and then click **Create**.

### To configure the WiFi user group - web-based manager

1. Go to **User & Device > User Groups** and select **Create New**.
2. Enter the following information and then select **OK**:

<b>Name</b>	wlan_users
<b>Type</b>	<b>Firewall</b>
<b>Members</b>	Add users.

### To configure a WiFi user and the WiFi user group - CLI

```
config user user
  edit "user01"
```

```

        set type password
        set passwd "asdf12ghjk"
    end
    config user group
        edit "wlan_users"
            set member "user01"
        end
    end

```

## Configuring the SSID

First, establish the SSID (network interface) for the network. This is independent of the number of physical access points that will be deployed. The network assigns IP addresses using DHCP.

### To configure the SSID - web-based manager

1. Go to **WiFi & Switch Controller > SSID** and select **Create New > SSID**.
2. Enter the following information and select **OK**:

<b>Interface Name</b>	example_wifi_if
<b>Traffic Mode</b>	Tunnel to Wireless Controller
<b>IP/Network Mask</b>	10.10.110.1/24
<b>Administrative Access</b>	Ping (to assist with testing)
<b>DHCP Server</b>	Enable
<b>Address Range</b>	10.10.110.2 - 10.10.110.199
<b>Netmask</b>	255.255.255.0
<b>Default Gateway</b>	Same As Interface IP
<b>DNS Server</b>	Same as System DNS
<b>SSID</b>	example_wifi
<b>Security Mode</b>	WPA2 Enterprise
<b>Authentication</b>	Local, select <b>wlan_users</b> user group.
Leave other settings at their default values.	

### To configure the SSID - CLI

```

config wireless-controller vap
    edit example_wifi_if
        set ssid "example_wifi"
        set broadcast-ssid enable
        set security wpa-enterprise
        set auth usergroup
        set usergroup wlan_users
        set schedule always
    end
config system interface

```

```

edit example_wifi_if
    set ip 10.10.110.1 255.255.255.0
end
config system dhcp server
    edit 0
        set default-gateway 10.10.110.1
        set dns-service default
        set interface "example_wifi_if"
        config ip-range
            edit 1
                set end-ip 10.10.110.199
                set start-ip 10.10.110.2
            end
        set netmask 255.255.255.0
    end
end

```

## Adding the SSID to the FortiAP Profile

The radio portion of the FortiAP configuration is contained in the FortiAP Profile. By default, there is a profile for each platform (FortiAP model). You can create additional profiles if needed. The SSID needs to be specified in the profile.

### To add the SSID to the FortiAP Profile - web-based manager

1. Go to **WiFi & Switch Controller > FortiAP Profiles** and edit the profile for your model of FortiAP unit.
2. In **Radio 1** and **Radio 2**, add example\_wifi in **SSID**.
3. Select **OK**.

## Configuring security policies

A security policy is needed to enable WiFi users to access the Internet on port1. First you create firewall address for the WiFi network, then you create the example\_wifi to port1 policy.

### To create a firewall address for WiFi users - web-based manager

1. Go to **Policy & Objects > Addresses**.
2. Select **Create New > Address**, enter the following information and select **OK**.

<b>Name</b>	wlan_user_net
<b>Type</b>	IP/Netmask
<b>Subnet / IP Range</b>	10.10.110.0/24
<b>Interface</b>	example_wifi_if
<b>Show in Address List</b>	Enabled

### To create a firewall address for WiFi users - CLI

```

config firewall address
    edit "wlan_user_net"
        set associated-interface "example_wifi_if"
    end
end

```

```
set subnet 10.10.110.0 255.255.255.0
end
```

### To create a security policy for WiFi users - web-based manager

1. Go to **Policy & Objects > IPv4 Policy** and select **Create New**.
2. Enter the following information and select **OK**:

<b>Incoming Interface</b>	example_wifi_if
<b>Source Address</b>	wlan_user_net
<b>Outgoing Interface</b>	port1
<b>Destination Address</b>	All
<b>Schedule</b>	always
<b>Service</b>	ALL
<b>Action</b>	ACCEPT
<b>NAT</b>	ON. Select <b>Use Destination Interface Address</b> (default).
Leave other settings at their default values.	

### To create a firewall policy for WiFi users - CLI

```
config firewall policy
edit 0
set srcintf "example_wifi"
set dstintf "port1"
set srcaddr "wlan_user_net"
set dstaddr "all"
set schedule always
set service ALL
set action accept
set nat enable
end
```

## Connecting the FortiAP units

You need to connect each FortiAP unit to the FortiGate unit, wait for it to be recognized, and then assign it to the AP Profile. But first, you must configure the interface to which the FortiAP units connect and the DHCP server that assigns their IP addresses.

In this example, the FortiAP units connect to port 3 and are controlled through IP addresses on the 192.168.8.0/24 network.

### To configure the interface for the AP unit - web-based manager

1. Go to **Network > Interfaces** and edit the port3 interface.
2. Set the **Addressing mode** to **Dedicated to Extension Device** and set the **IP/Network Mask** to

```
192.168.8.1/255.255.255.0.
```

### 3. Select **OK**.

This procedure automatically configures a DHCP server for the AP units.

#### To configure the interface for the AP unit - CLI

```
config system interface
edit port3
set mode static
set ip 192.168.8.1 255.255.255.0
end
```

#### To configure the DHCP server for AP units - CLI

```
config system dhcp server
edit 0
set interface port3
config exclude-range
edit 1
set end-ip 192.168.8.1
set start-ip 192.168.8.1
end
config ip-range
edit 1
set end-ip 192.168.8.254
set start-ip 192.168.8.2
end
set netmask 255.255.255.0
set vci-match enable
set vci-string "FortiAP"
end
```

#### To connect a FortiAP unit - web-based manager

1. Go to **WiFi & Switch Controller > Managed FortiAPs**.
2. Connect the FortiAP unit to port 3.
3. Periodically select **Refresh** while waiting for the FortiAP unit to be listed.  
Recognition of the FortiAP unit can take up to two minutes.  
If FortiAP units are connected but cannot be recognized, try disabling VCI-Match in the DHCP server settings.
4. When the FortiAP unit is listed, select the entry to edit it.  
The **Edit Managed Access Point** window opens.
5. In **State**, select **Authorize**.
6. In **FortiAP Profile**, select the default profile for the FortiAP model.
7. Select **OK**.
8. Repeat Steps 2 through 8 for each FortiAP unit.

#### To connect a FortiAP unit - CLI

1. Connect the FortiAP unit to port 3.
2. Enter

```
config wireless-controller wtp
```

3. Wait 30 seconds, then enter `get`.

Retry the `get` command every 15 seconds or so until the unit is listed, like this:

```
== [ FAP22B3U10600118 ]  
wtp-id: FAP22B3U10600118
```

4. Edit the discovered FortiAP unit like this:

```
edit FAP22B3U10600118  
  set admin enable  
end
```

5. Repeat Steps 2 through 4 for each FortiAP unit.

## A more complex example

This example creates multiple networks and uses custom AP profiles.

### Scenario

In this example, Example Co. provides two wireless networks, one for its employees and the other for customers or other guests of its business. Guest users have access only to the Internet, not to the company's private network. The equipment for these WiFi networks consists of FortiAP-220B units controlled by a FortiGate unit.

The employee network operates in 802.11n mode on both the 2.4GHz and 5GHz bands. Client IP addresses are in the 10.10.120.0/24 subnet, with 10.10.120.1 the IP address of the WAP. The guest network also operates in 802.11n mode, but only on the 2.4GHz band. Client IP addresses are on the 10.10.115.0/24 subnet, with 10.10.115.1 the IP address of the WAP.

On FortiAP-220B units, the 802.11n mode also supports 802.11g and 802.11b clients on the 2.4GHz band and 802.11a clients on the 5GHz band.

The guest network WAP broadcasts its SSID, the employee network WAP does not.

The employees network uses WPA-Enterprise authentication through a FortiGate user group. The guest network features a captive portal. When a guest first tries to connect to the Internet, a login page requests logon credentials. Guests use numbered guest accounts authenticated by RADIUS. The captive portal for the guests includes a disclaimer page.

In this example, the FortiAP units connect to port 3 and are assigned addresses on the 192.168.8.0/24 subnet.

### Configuration

To configure these wireless networks, you must:

- Configure authentication for wireless users
- Configure the SSIDs (network interfaces)
- Configure the AP profile
- Configure the WiFi LAN interface and a DHCP server
- Configure firewall policies

## Configuring authentication for employee wireless users

Employees have user accounts on the FortiGate unit. This example shows creation of one user account, but you can create multiple accounts and add them as members to the user group.

### To configure a WiFi user - web-based manager

1. Go to **User & Device > User Definition** and select **Create New**.
2. Select **Local User** and then click **Next**.
3. Enter a **User Name** and **Password** and then click **Next**.
4. Click **Next**.
5. Make sure that **Enable** is selected and then click **Create**.

### To configure the user group for employee access - web-based manager

1. Go to **User & Device > User Groups** and select **Create New**.
2. Enter the following information and then select **OK**:

<b>Name</b>	employee-group
<b>Type</b>	Firewall
<b>Members</b>	Add users.

### To configure a WiFi user and the user group for employee access - CLI

```
config user user
  edit "user01"
    set type password
    set passwd "asdf12ghjk"
  end
config user group
  edit "employee-group"
    set member "user01"
  end
```

The user authentication setup will be complete when you select the employee-group in the SSID configuration.

## Configuring authentication for guest wireless users

Guests are assigned temporary user accounts created on a RADIUS server. The RADIUS server stores each user's group name in the Fortinet-Group-Name attribute. Wireless users are in the group named "wireless".

The FortiGate unit must be configured to access the RADIUS server.

### To configure the FortiGate unit to access the guest RADIUS server - web-based manager

1. Go to **User & Device > RADIUS Servers** and select **Create New**.
2. Enter the following information and select OK:

<b>Name</b>	guestRADIUS
<b>Primary Server IP/Name</b>	10.11.102.100
<b>Primary Server Secret</b>	grikfwpdfg
<b>Secondary Server IP/Name</b>	Optional
<b>Secondary Server Secret</b>	Optional
<b>Authentication Scheme</b>	Use default, unless server requires otherwise.
Leave other settings at their default values.	

### To configure the FortiGate unit to access the guest RADIUS server - CLI

```
config user radius
  edit guestRADIUS
    set auth-type auto
    set server 10.11.102.100
    set secret grikfwpdfg
  end
```

### To configure the user group for guest access - web-based manager

1. Go to **User & Device > User Groups** and select **Create New**.
2. Enter the following information and then select **OK**:

<b>Name</b>	guest-group
<b>Type</b>	<b>Firewall</b>
<b>Members</b>	Leave empty.

3. Select **Create new**.
4. Enter:

<b>Remote Server</b>	Select <b>guestRADIUS</b> .
<b>Groups</b>	Select <b>wireless</b>

5. Select **OK**.

### To configure the user group for guest access - CLI

```
config user group
  edit "guest-group"
    set member "guestRADIUS"
    config match
      edit 0
        set server-name "guestRADIUS"
        set group-name "wireless"
      end
    end
end
```



The user authentication setup will be complete when you select the guest-group user group in the SSID configuration.

## Configuring the SSIDs

First, establish the SSIDs (network interfaces) for the employee and guest networks. This is independent of the number of physical access points that will be deployed. Both networks assign IP addresses using DHCP.

### To configure the employee SSID - web-based manager

1. Go to **WiFi & Switch Controller > SSID** and select **Create New > SSID**.
2. Enter the following information and select **OK**:

<b>Interface Name</b>	example_inc
<b>Traffic Mode</b>	Tunnel to Wireless Controller
<b>IP/Netmask</b>	10.10.120.1/24
<b>Administrative Access</b>	Ping (to assist with testing)
<b>Enable DHCP</b>	Enable
<b>Address Range</b>	10.10.120.2 - 10.10.120.199
<b>Netmask</b>	255.255.255.0
<b>Default Gateway</b>	Same As Interface IP
<b>DNS Server</b>	Same as System DNS
<b>SSID</b>	example_inc
<b>Security Mode</b>	WPA/WPA2-Enterprise
<b>Authentication</b>	Select <b>Local</b> , then select <b>employee-group</b> .
Leave other settings at their default values.	

### To configure the employee SSID - CLI

```
config wireless-controller vap
  edit example_inc
    set ssid "example_inc"
    set security wpa-enterprise
    set auth usergroup
    set usergroup employee-group
    set schedule always
  end
config system interface
  edit example_inc
    set ip 10.10.120.1 255.255.255.0
  end
config system dhcp server
  edit 0
```

```

set default-gateway 10.10.120.1
set dns-service default
set interface example_inc
config ip-range
  edit 1
    set end-ip 10.10.120.199
    set start-ip 10.10.120.2
  end
set lease-time 7200
set netmask 255.255.255.0
end

```

### To configure the example\_guest SSID - web-based manager

1. Go to **WiFi & Switch Controller > SSID** and select **Create New**.
2. Enter the following information and select **OK**:

<b>Name</b>	example_guest
<b>IP/Netmask</b>	10.10.115.1/24
<b>Administrative Access</b>	Ping (to assist with testing)
<b>Enable DHCP</b>	Enable
<b>Address Range</b>	10.10.115.2 - 10.10.115.50
<b>Netmask</b>	255.255.255.0
<b>Default Gateway</b>	Same as Interface IP
<b>DNS Server</b>	Same as System DNS
<b>SSID</b>	example_guest
<b>Security Mode</b>	Captive Portal
<b>Portal Type</b>	Authentication
<b>Authentication Portal</b>	Local
<b>User Groups</b>	Select <b>guest-group</b>
Leave other settings at their default values.	

### To configure the example\_guest SSID - CLI

```

config wireless-controller vap
  edit example_guest
    set ssid "example_guest"
    set security captive-portal
    set selected-usergroups guest-group
    set schedule always
  end
config system interface
  edit example_guest
    set ip 10.10.115.1 255.255.255.0
  end

```

```

end
config system dhcp server
edit 0
set default-gateway 10.10.115.1
set dns-service default
set interface "example_guest"
config ip-range
edit 1
set end-ip 10.10.115.50
set start-ip 10.10.115.2
end
set lease-time 7200
set netmask 255.255.255.0
end

```

## Configuring the FortiAP profile

The FortiAP Profile defines the radio settings for the networks. The profile provides access to both Radio 1 (2.4GHz) and Radio 2 (5GHz) for the employee virtual AP, but provides access only to Radio 1 for the guest virtual AP.

### To configure the FortiAP Profile - web-based manager

1. Go to **WiFi & Switch Controller > FortiAP Profiles** and select **Create New**.
2. Enter the following information and select **OK**:

<b>Name</b>	example_AP
<b>Platform</b>	FAP220B
<b>Radio 1</b>	
<b>Mode</b>	Access Point
<b>Band</b>	802.11n
<b>Channel</b>	Select 1, 6, and 11.
<b>Tx Power</b>	100%
<b>SSID</b>	<b>Select SSIDs</b> and select <b>example_inc</b> and <b>example_guest</b> .
<b>Radio 2</b>	
<b>Mode</b>	Access Point
<b>Band</b>	802.11n_5G
<b>Channel</b>	Select all.
<b>Tx Power</b>	100%
<b>SSID</b>	<b>Select SSIDs</b> and select <b>example_inc</b> .

### To configure the AP Profile - CLI

```

config wireless-controller wtp-profile
  edit "example_AP"
    config platform
      set type 220B
    end
    config radio-1
      set ap-bgscan enable
      set band 802.11n
      set channel "1" "6" "11"
      set vaps "example_inc" "example_guest"
    end
    config radio-2
      set ap-bgscan enable
      set band 802.11n-5G
      set channel "36" "40" "44" "48" "149" "153" "157" "161" "165"
      set vaps "example_inc"
    end
  end
end

```

## Configuring firewall policies

Identity-based firewall policies are needed to enable the WLAN users to access the Internet on Port1. First you create firewall addresses for employee and guest users, then you create the firewall policies.

### To create firewall addresses for employee and guest WiFi users

1. Go to **Policy & Objects > Addresses**.
2. Select **Create New**, enter the following information and select **OK**.

<b>Address Name</b>	employee-wifi-net
<b>Type</b>	Subnet / IP Range
<b>Subnet / IP Range</b>	10.10.120.0/24
<b>Interface</b>	example_inc

3. Select **Create New**, enter the following information and select **OK**.

<b>Address Name</b>	guest-wifi-net
<b>Type</b>	Subnet / IP Range
<b>Subnet / IP Range</b>	10.10.115.0/24
<b>Interface</b>	example_guest

### To create firewall policies for employee WiFi users - web-based manager

1. Go to **Policy & Objects > IPv4 Policy** and select **Create New**.
2. Enter the following information and select **OK**:

<b>Incoming Interface</b>	example_inc
<b>Source Address</b>	employee-wifi-net
<b>Outgoing Interface</b>	port1
<b>Destination Address</b>	all
<b>Schedule</b>	always
<b>Service</b>	ALL
<b>Action</b>	ACCEPT
<b>NAT</b>	Enable NAT

3. Optionally, select security profile for wireless users.
4. Select **OK**.
5. Repeat steps 1 through 4 but select Internal as the Destination Interface/Zone to provides access to the ExampleCo private network.

#### To create firewall policies for employee WiFi users - CLI

```
config firewall policy
  edit 0
    set srcintf "employee_inc"
    set dstintf "port1"
    set srcaddr "employee-wifi-net"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ANY"
    set nat enable
    set schedule "always"
    set service "ANY"
  next
  edit 0
    set srcintf "employee_inc"
    set dstintf "internal"
    set srcaddr "employee-wifi-net"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ANY"
    set nat enable
    set schedule "always"
    set service "ANY"
  end
```

#### To create a firewall policy for guest WiFi users - web-based manager

1. Go to **Policy & Objects > IPv4 Policy** and select **Create New**.
2. Enter the following information and select **OK**:

<b>Incoming Interface</b>	example_guest
<b>Source Address</b>	guest-wifi-net
<b>Outgoing Interface</b>	port1
<b>Destination Address</b>	all
<b>Schedule</b>	always
<b>Service</b>	ALL
<b>Action</b>	ACCEPT
<b>NAT</b>	Enable NAT

3. Optionally, select **UTM** and set up UTM features for wireless users.
4. Select **OK**.

#### To create a firewall policy for guest WiFi users - CLI

```
config firewall policy
  edit 0
    set srcintf "example_guest"
    set dstintf "port1"
    set srcaddr "guest-wifi-net"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ANY"
    set nat enable
  end
```

## Connecting the FortiAP units

You need to connect each FortiAP-220A unit to the FortiGate unit, wait for it to be recognized, and then assign it to the AP Profile. But first, you must configure the interface to which the FortiAP units connect and the DHCP server that assigns their IP addresses.

In this example, the FortiAP units connect to port 3 and are controlled through IP addresses on the 192.168.8.0/24 network.

#### To configure the interface for the AP unit - web-based manager

1. Go to **Network > Interfaces** and edit the port3 interface.
2. Set the **Addressing mode** to **Dedicated to Extension Device** and set the **IP/Netmask** to 192.168.8.1/255.255.255.0.  
This step automatically configures a DHCP server for the AP units.
3. Select **OK**.

#### To configure the interface for the AP unit - CLI

```
config system interface
  edit port3
```

```

set mode static
set ip 192.168.8.1 255.255.255.0
end

```

### To configure the DHCP server for AP units - CLI

```

config system dhcp server
edit 0
set interface port3
config ip-range
edit 1
set end-ip 192.168.8.9
set start-ip 192.168.8.2
end
set netmask 255.255.255.0
set vci-match enable
set vci-string "FortiAP"
end

```

### To connect a FortiAP-220A unit - web-based manager

1. Go to **WiFi & Switch Controller > Managed FortiAPs**.
2. Connect the FortiAP unit to port 3.
3. Periodically select **Refresh** while waiting for the FortiAP unit to be listed.  
Recognition of the FortiAP unit can take up to two minutes.  
If there is persistent difficulty recognizing FortiAP units, try disabling VCI-Match in the DHCP server settings.
4. When the FortiAP unit is listed, select the entry to edit it.  
The **Edit Managed Access Point** window opens.
5. In **State**, select **Authorize**.
6. In the **AP Profile**, select **[Change]** and then select the **example\_AP** profile.
7. Select **OK**.
8. Repeat Steps 2 through 8 for each FortiAP unit.

### To connect a FortiAP-220A unit - CLI

1. Connect the FortiAP unit to port 3.
2. Enter:  

```
config wireless-controller wtp
```
3. Wait 30 seconds, then enter `get`.  
Retry the `get` command every 15 seconds or so until the unit is listed, like this:

```

== [ FAP22A3U10600118 ]
wtp-id: FAP22A3U10600118

```

4. Edit the discovered FortiAP unit like this:  

```
edit FAP22A3U10600118
set admin enable
set wtp-profile example_AP
end
```
5. Repeat Steps 2 through 4 for each FortiAP unit.

# Managing a FortiAP with FortiCloud

This chapter provides a few FortiCloud-managed FortiAP configuration examples.

FortiCloud-managed FortiAP WiFi

FortiCloud-managed FortiAP WiFi without a key

You can register for a free FortiCloud account at [www.forticloud.com](http://www.forticloud.com).

For a video tutorial of how to configure and manage a FortiAP-S device from FortiCloud, follow the link below:

- [How to configure and Manage FortiAP-S from FortiCloud](#)

## FortiCloud-managed FortiAP WiFi

In this example, you use FortiCloud to configure a single FortiAP-221C, creating a working WiFi network without a FortiGate.

FortiCloud remote management is supported on FortiAP models 221C and 320C.

For this configuration, the FortiAP-221C unit is running version 5.2 firmware. You will create a simple network that uses WPA-Personal authentication.

You can register for a free FortiCloud account at [www.forticloud.com](http://www.forticloud.com).

To create the WiFi network without a FortiGate unit, you must:

- Add your FortiAP to FortiCloud
- Configure the SSID
- Configure the AP platform profile
- Deploy the AP with the profile

## Adding your FortiAP to FortiCloud

You need to add the FortiAP unit to your FortiCloud account. This is done through a unique key that can be found under the FortiAP unit.

### To add a FortiAP to FortiCloud

1. Connect the FortiAP Ethernet interface to a network that provides access to the Internet.
2. Open a web browser and navigate to the FortiCloud main page and select **+ AP Network**.
3. Enter an **AP Network Name** and **AP Password**. This password is used to locally log in to the AP as the administrator. It will be set to all APs in this AP network.
4. Set the correct **Time Zone** and select **Submit**.

## Configuring the SSID

You must establish the SSID (network interface) for the WiFi network.



### To configure the SSID

1. Select the FortiAP you just created from the home page. You will then be prompted to add an SSID for the AP Network.  
In the interface, this is under **Configure > SSIDs**.
2. In **Access Control**, enter the name of your SSID, set **Authentication** to **WPA2-Personal**, enter the **Pre-shared Key**, and select **Next**.
3. In **Security**, enable security features as required (select from **AntiVirus**, **Intrusion Prevention**, **Block Botnet**, **Web Access**, and **Application Control**) and select **Next**.
4. In **Availability**, make sure to leave **5 GHz** enabled, configure a schedule as required, and select **Next**.
5. Review your SSID in **Preview**, then select **Apply**.

## Configuring the AP platform profile

The radio portion of the FortiAP configuration is contained in the FortiAP platform profile. By default, there is a profile for each platform (FortiAP model). The SSID needs to be specified in the profile.

### To configure the AP profile

1. Go to **Configure > AP Profile** and edit the AP Profile for your FortiAP model (mouse-over the AP Profile to reveal the **Edit** button).
2. Enable the SSID configured earlier for both **Radio 1** and **Radio 2**, for 5GHz coverage.

## Deploying the AP with the platform profile

With the SSID and platform profile configured, you must deploy the AP by entering the FortiCloud key for the FortiAP.

### To deploy the AP

1. Go to **Configure > Deploy APs**. Here you will be prompted to enter the FortiCloud key, which can be found on the same label as the FortiAP unit's serial number, and select **Submit**.



If you have a FortiAP model that does *not* include a FortiCloud key, you can still add the device to the network. To learn how, see the [FortiCloud-managed FortiAP WiFi without a key](#) configuration.

---

2. In **Set Platform Profiles**, select the platform profile you created earlier and select **Next**.
3. Follow the rest of the deployment wizard. Select **Submit** when completed.

You will now be able to connect to the wireless network and browse the Internet. On the FortiCloud website, go to **Monitor > Report** where you can view monitoring information such as **Traffic by Period**, **Client Count by Period**, and more.

## FortiCloud-managed FortiAP WiFi without a key

You can manage your FortiAP-based wireless network with FortiCloud even if your FortiAP has no FortiCloud key.

For this example, you will need to have already pre-configured your FortiAP unit with your FortiCloud account credentials. For more information on how to do this, or if your FortiAP has a FortiCloud key (on the serial number label), see the [FortiCloud-managed FortiAP WiFi](#) configuration.

You can register for a free FortiCloud account at [www.forticloud.com](http://www.forticloud.com).

To create the WiFi network without a FortiCloud key, you must:

- Configure the FortiAP unit
- Add the FortiAP unit to your FortiCloud account
- Configure the FortiAP

## Configuring the FortiAP unit

You need to connect and configure the FortiAP unit through the web-based manager of the FortiGate.

### To configure the FortiAP unit - web-based manager

1. Connect your computer to the FortiAP Ethernet port. The FortiAP's default IP address is 192.168.1.2. The computer should have an address on the same subnet, 192.168.1.3 for example.
2. Using a browser, log in to the FortiAP as *admin*. Leave the password field empty.
3. In **WTP-Configuration**, select **FortiCloud** and enter your FortiCloud credentials. Select **Apply**.  
The FortiAP is now ready to connect to FortiCloud via the Internet.

## Adding the FortiAP unit to your FortiCloud account

The FortiAP must be added to the FortiCloud account that has a WiFi network already configured for it.

For an example of creating a WiFi network on FortiCloud, see [FortiCloud-managed FortiAP WiFi on page 152](#).

### To add the FortiAP to FortiCloud

1. Connect the FortiAP Ethernet cable to a network that connects to the Internet.  
Restore your computer to its normal network configuration and log on to FortiCloud.
2. From the **Home** screen, go to **Inventory > AP Inventory**. Your FortiAP should be listed.
3. Then go back to the Home screen, select your AP network, and go to **Deploy APs**.
4. Select your listed FortiAP and select **Next**.
5. Make sure your platform profile is selected from the dropdown menu, and select **Next**.
6. In **Preview**, select **Deploy**.

The device will now appear listed under **Access Points**.

You will now be able to connect to the wireless network and browse the Internet. On the FortiCloud website, go to **Monitor > Report** where you can view monitoring information such as **Traffic by Period**, **Client Count by Period**, and more.

# Using a FortiWiFi unit as a client

A FortiWiFi operates by default as a wireless access point. But a FortiWiFi can also operate as a wireless client, connecting the FortiGate to another wireless network.

[Use of client mode](#)

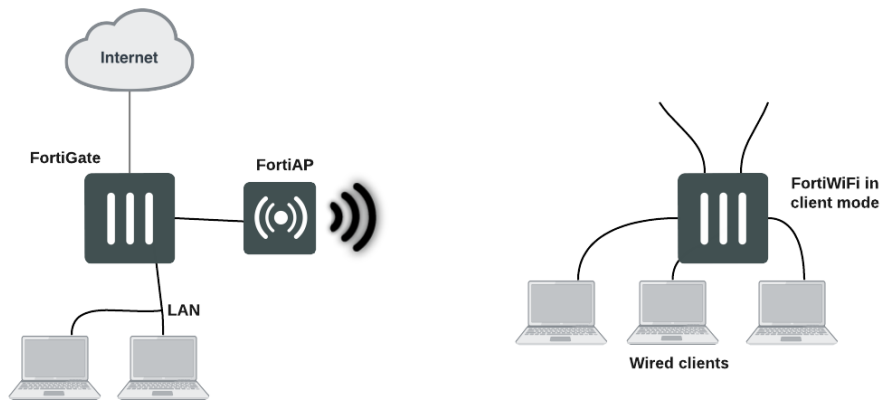
[Configuring client mode](#)

## Use of client mode

In client mode, the FortiWiFi unit connects to a remote WiFi access point to access other networks or the Internet. This is most useful when the FortiWiFi unit is in a location that does not have a wired infrastructure.

For example, in a warehouse where shipping and receiving are on opposite sides of the building, running cables might not be an option due to the warehouse environment. The FortiWiFi unit can support wired users using its Ethernet ports and can connect to another access point wirelessly as a client. This connects the wired users to the network using the 802.11 WiFi standard as a backbone.

Note that in client mode the FortiWiFi unit cannot operate as an AP. WiFi clients cannot see or connect to the FortiWiFi unit in Client mode.

**FortiWiFi unit in Client mode**

## Configuring client mode

To set up the FortiAP unit as a WiFi client, you must use the CLI. Before you do this, be sure to remove any AP WiFi configurations such as SSIDs, DHCP servers, policies, and so on.

### To configure wireless client mode

1. Change the WiFi mode to client.

In the CLI, enter the following commands:

```
config system global
    set wireless-mode client
end
```

Respond "y" when asked if you want to continue. The FortiWiFi unit will reboot.

2. Configure the WiFi interface settings.

For example, to configure the client for WPA-Personal authentication on the **our\_wifi** SSID with passphrase **justforus**, enter the following in the CLI:

```
config system interface
    edit wifi
        set mode dhcp
        config wifi-networks
            edit 0
                set wifi-ssid our_wifi
                set wifi-security wpa-personal
                set wifi-passphrase "justforus"
            end
        end
    end
```

The WiFi interface client\_wifi will receive an IP address using DHCP.

3. Configure a wifi to port1 policy.

You can use either CLI or web-based manager to do this. The important settings are:

<b>Incoming Interface (srcintf)</b>	wifi
<b>Source Address (srcaddr)</b>	all
<b>Outgoing Interface (dstintf)</b>	port1
<b>Destination Address (dstaddr)</b>	all
<b>Schedule</b>	always
<b>Service</b>	ALL
<b>Action</b>	ACCEPT
<b>Enable NAT</b>	Selected

## Controlled AP selection support in FWF client mode

Use the following CLI commands to provide a more controlled AP selection method (supported in FortiWiFi client mode).

### Syntax

```
config system interface
  edit {name}
    set wifi-ap-band {any | 5g-preferred | 5g-only}
  next
end
```

# Support for location-based services

FortiOS supports location-based services by collecting information about WiFi devices near FortiGate-managed access points, even if the devices don't associate with the network.

[Overview](#)

[Configuring location tracking](#)

[Viewing device location data on the FortiGate unit](#)

## Overview

WiFi devices broadcast packets as they search for available networks. The FortiGate WiFi controller can collect information about the interval, duration, and signal strength of these packets. The Euclid Analytics service uses this information to track the movements of the device owner. A typical application of this technology is to analyze shopper behavior in a shopping center. Which stores do people walk past? Which window displays do they stop to look at? Which stores do they enter and how long do they spend there? The shoppers are not personally identified, each is known only by the MAC address of their WiFi device.

After enabling location tracking on the FortiGate unit, you can confirm that the feature is working by using a specialized diagnostic command to view the raw tracking data. The Euclid Analytics service obtains the same data in its proprietary format using a JSON inquiry through the FortiGate unit's web-based manager interface.

## Configuring location tracking

You can enable location tracking in any FortiAP profile, using the CLI. Location tracking is part of location-based services. Set the `station-locate` field to `enable`. For example:

```
config wireless-controller wtp-profile
  edit "FAP220B-locate"
    set ap-country US
    config platform
      set type 220B
    end
    config lbs
      set station-locate enable
    end
  end
end
```

## Automatic deletion of outdated presence data

The FortiGate generates a log entry only the first time that station-locate detects a mobile client. No log is generated for clients that have been detected before. To log repeat client visits, previous station presence data must be deleted (flushed). The `sta-locate-timer` can flush this data periodically. The default period is 1800 seconds (30 minutes). The timer can be set to any value between 1 and 86400 seconds (24 hours). A setting of 0 disables the flush, meaning a client is logged only on the very first visit.

The timer is one of the wireless controller timers and it can be set in the CLI. For example:

```
config wireless-controller timers
  set sta-locate-timer 1800
end
```

The sta-locate-timer should not be set to less than the sta-capability-timer (default 30 seconds) because that could cause duplicate logs to be generated.

## FortiPresence push REST API

When the FortiGate is located on a private IP network, the FortiPresence server cannot poll the FortiGate for information. Instead, the FortiGate must be configured to push the information to the FortiPresence server.

Enter the following command:

```
config wireless-controller wtp-profile
  edit "FP223B-GuestWiFi"
    config lbs
      set fortipresence {enable | disable}
      set fortipresence-server <ip-address> Default is 3000.
      set fortipresence-port <port>
      set fortipresence-secret <password>
      set fortipresence-project <name>
      set fortipresence-frequency <5-65535> Default is 30.
      set fortipresence-rogue {enable | disable} Enable/disable reporting of Rogue APs.
      set fortipresence-unassoc {enable | disable} Enable/disable reporting of unassociated devices.
    end
  end
end
```

## Viewing device location data on the FortiGate unit

You can use the FortiGate CLI to list located devices. This is mainly useful to confirm that the location data feature is working. You can also reset device location data.

### To list located devices

```
diag wireless-controller wlac -c sta-locate
```

### To reset device location data

```
diag wireless-controller wlac -c sta-locate-reset
```

## Example output

The following output shows data for three WiFi devices.

```
FWF60C3G11004319 # diagnose wireless-controller wlac -c sta-locate
sta_mac vfid rid base_mac freq_lst frm_cnt frm_fst frm_last intv_sum intv2_sum intv3_
sum intv_min intv_max signal_sum signal2_sum signal3_sum sig_min sig_max sig_fst
sig_last ap

00:0b:6b:22:82:61 0
FAP22B3U11005354 0 0 00:09:0f:f1:bb:e4 5745 257 708 56 651 1836 6441 0 12 -21832
1855438 -157758796 -88 -81 -84 -88 0
```



```
00:db:df:24:1a:67 0
FAP22B3U11005354 0 0 00:09:0f:f1:bb:e4 5745 42 1666 41 1625 97210 5831613 0 60 -3608
310072 -26658680 -90 -83 -85 -89 0

10:68:3f:50:22:29 0
FAP22B3U11005354 0 0 00:09:0f:f1:bb:e4 5745 102 1623 58 1565 94136 5664566 0 60 -8025
631703 -49751433 -84 -75 -78 -79 0
```

The output for each device appears on two lines. The first line contains only the device MAC address and the VLAN ID. The second line begins with the ID (serial number) of the FortiWiFi or FortiAP unit that detected the device, the AP's MAC address, and then the fields that the Euclid service uses. Because of its length, this line wraps around and displays as multiple lines.

# Troubleshooting

In the following section, you will learn basic troubleshooting techniques for a secure Fortinet wireless LAN including:

- strategies for troubleshooting Fortinet wireless devices
- how to avoid common misconfigurations
- solutions to connectivity issues
- capturing and analyzing wireless traffic
- wireless debug commands

The goal of this document is to provide you with practical knowledge that you can use to troubleshoot the FortiOS wireless controller and FortiAP devices. This includes how to use tools and apply CLI commands for maintenance and troubleshooting of your wireless network infrastructure, analyze problems per OSI layer, explore diagnostics for commissioning issues regarding at-client and access point connectivity problems, and understand the packet sniffer technique as a strong troubleshooting tool.

The content is divided as follows:

[FortiAP shell command through CAPWAP control tunnel](#)

[Signal strength issues](#)

[Throughput issues](#)

[Connection issues](#)

[General problems](#)

[Packet sniffer](#)

[Useful debugging commands](#)

## FortiAP shell command through CAPWAP control tunnel

Very often, the FortiAP in the field is behind a NAT device, and access to the FortiAP through Telnet or SSH is not available. As a troubleshooting enhancement, this feature allows an AP shell command up to 127-bytes sent to the FAP, and FAP will run this command, and return the results to the controller using the CAPWAP tunnel.

The maximum output from a command is limited to 4M, and the default output size is set to 32K.

The FortiAP will only report running results to the controller after the command is finished. If a new command is sent to the AP before the previous command is finished, the previous command will be canceled.

Enter the following:

```
diag w-c wlac wtpcmd wtp_ip wtp_port cmd [cmd-to-ap] cmd: run,show,showhex,clr,r&h,r&sh
```

- **cmd-to-ap:** any shell commands, but AP will not report results until the command is finished on the AP
- **run:** controller sends the ap-cmd to the FAP to run
- **show:** show current results reported by the AP in text
- **showhex:** show current results reported by the AP in hex
- **clr:** clear reported results

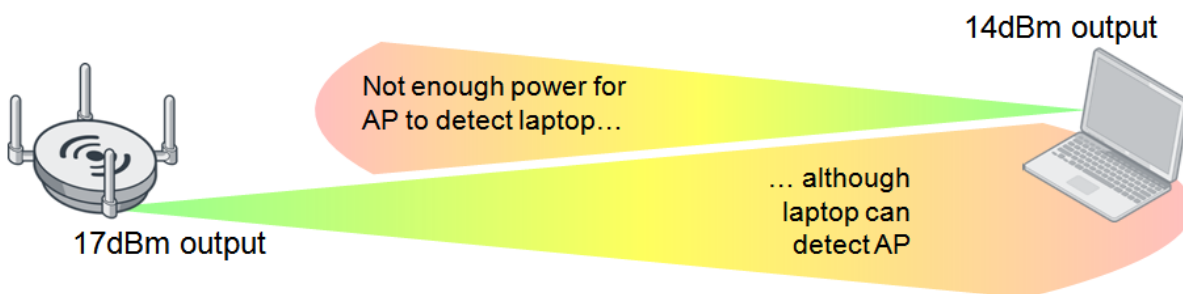
- **r&s:** run/show
- **r&sh:** run/showhex

## Signal strength issues

Poor signal strength is possibly the most common customer complaint. Below you will learn where to begin identifying and troubleshooting poor signal strength, and learn what information you can obtain from the customer to help resolve signal strength issues.

### Asymmetric power issue

Asymmetric power issues are a typical problem. Wireless is two-way communication; high power access points (APs) can usually transmit a long distance, however, the client's ability to transmit is usually not equal to that of the AP and, as such, cannot return transmission if the distance is too far.



### Measuring signal strength in both directions

To solve an asymmetric power issue, measure the signal strength in both directions. APs usually have enough power to transmit long distances, but sometimes battery-powered clients have a reply signal that has less power, and therefore the AP cannot detect their signal.

It is recommended that you match the transmission power of the AP to the least powerful wireless client—around 10 decibels per milliwatt (dBm) for iPhones and 14dBm for most laptops.

Even if the signal is strong enough, other devices may be emitting radiation as well, causing interference. To identify the difference, read the client Rx strength from the FortiGate GUI (under **Monitor > WiFi Client Monitor**) or CLI.

The **Signal Strength/Noise** value provides the received signal strength indicator (RSSI) of the wireless client. For example, A value of -85dBm to -95dBm is equal to about 10dB levels; this is not a desirable signal strength. In the following screenshot, one of the clients is at 18dB, which is getting close to the perimeter of its range.

SSID	FortiAP	IP	Device	Channel	Bandwidth Tx/Rx	Signal Strength/Noise	Signal
AP MavisF	FAP28C3X13000119 (1)	10.0.2.8	e8:91:20:90:6e:23	6	1 kbps	29 dB	■■■■■■■■■■
AP MavisF	FP320C3X14000668 (1)	192.168.255.112	1c:69:a5:c8:e8:3e	11	80 bps	35 dB	■■■■■■■■■■
AP MavisF	FP320C3X14000668 (2)	192.168.255.101	58:55:ca:36:28:7d	44	12 kbps	51 dB	■■■■■■■■■■
AP MavisF	FAP28C3X13000119 (1)	10.0.2.9	Acer A1-830 Tablet	6	543 bps	18 dB	■■■■■■■■■■
AP MavisF	FAP28C3X13000119 (1)	10.0.2.13	08:ed:b9:4f:98:ad	6	16 kbps	31 dB	■■■■■■■■■■
AP MavisF	FP320C3X14000668 (1)	192.168.255.115	Ellas_Tablet	11	0 bps	35 dB	■■■■■■■■■■



The Signal Strength/Noise value received from the FortiAP by clients, and vice versa, should be within the range of -20dBm to -65dBm.

---

You can also confirm the transmission (Tx) power of the controller on the AP profile (`wtp-profile`) and the FortiAP (`iwconfig`), and check the power management (auto-Tx) options.

#### Controller configured transmitting power - CLI:

```
config wireless-controller wtp-profile
config <radio>
show
(the following output is limited to power levels)
  auto-power-level : enable
  auto-power-high  : 17
  auto-power-low   : 10
```

#### Actual FortiAP transmitting power - CLI:

```
iwconfig wlan00
```

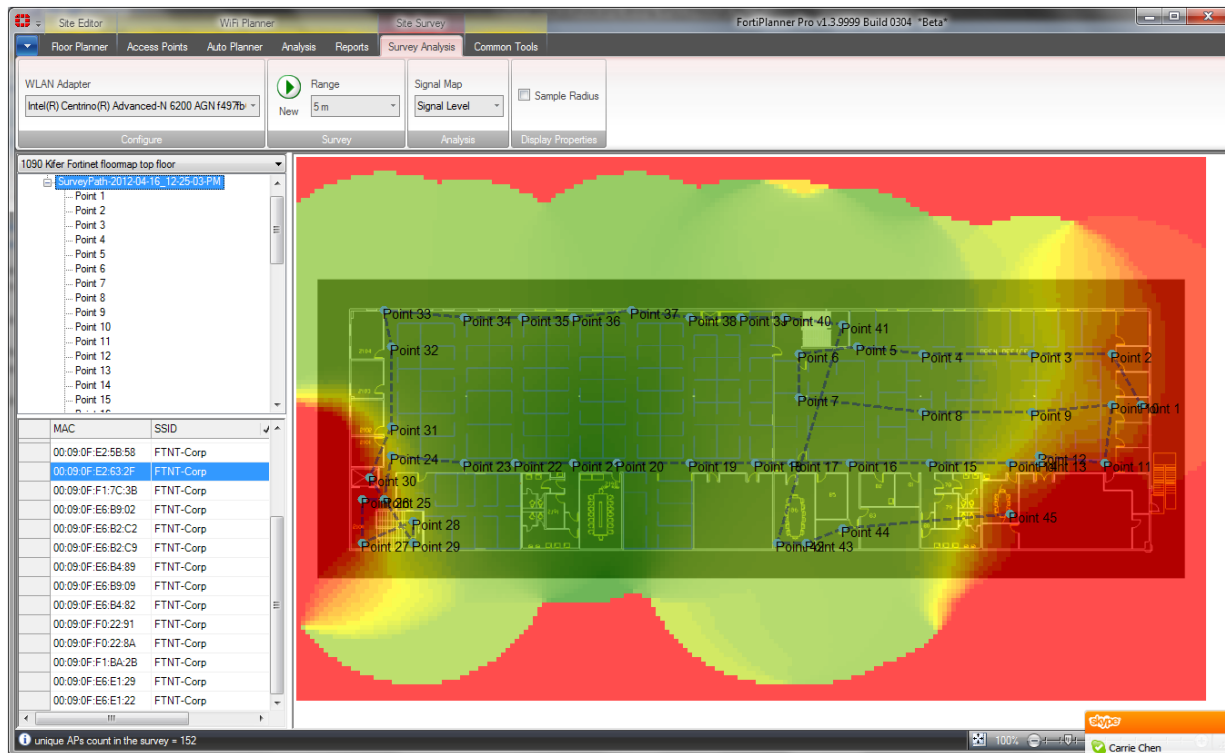
**Result:**

```
wlan00 IEEE 802.11ng ESSID:"signal-check"
Mode:Master Frequency:2.412 GHz   Access Point:<MAC add>
Bit Rate:130 Mb/s Tx-Power=28 dBm
```

### Using FortiPlanner PRO with a site survey

The most thorough method to solve signal strength issues is to perform a site survey. To this end, Fortinet offers the FortiPlanner, downloadable at [http://www.fortinet.com/resource\\_center/product\\_downloads.html](http://www.fortinet.com/resource_center/product_downloads.html).

## Sample depiction of a site survey using FortiPlanner



The site survey provides you with optimal placement for your APs based on the variables in your environment. You must provide the site survey detailed information including a floor plan (to scale), structural materials, and more. It will allow you to place the APs on the map and adjust the radio bands and power levels while providing you with visual wireless coverage.

Below is a list of mechanisms for gathering further information on the client for Rx strength. The goal is to see how well the client is receiving the signal from the AP. You can also verify FortiAP signal strength on the client using WiFi client utilities, or third party utilities such as InSSIDer or MetaGeek Chanalyzer. You can get similar tools from the app stores on Android and iOS devices.

- Professional Site Survey software (Ekahau, Airmagnet survey Pro, FortiPlanner)
- InSSIDer
- On Windows: `netsh wlan show networks mode=bssid` (look for the BSSID, it's in % not in dBm!)
- On MacOS: Use the `airport` command:  

```
"/System/Library/PrivateFrameworks/Apple80211.framework/Versions/A/Resources/airport" airport -s |
grep <the_bssid> (live scan each time)
```
- On Droid: WiFiFoFum

## Frequency interference

If the wireless signal seems to be strong but then periodically drops, this may be a symptom of frequency interference. Frequency interference is when another device also emits radio frequency using the same channel,

co-channel, or adjacent channel, thereby overpowering or corrupting your signal. This is a common problem on a 2.4GHz network.

There are two types of interference: coherent and non-coherent.

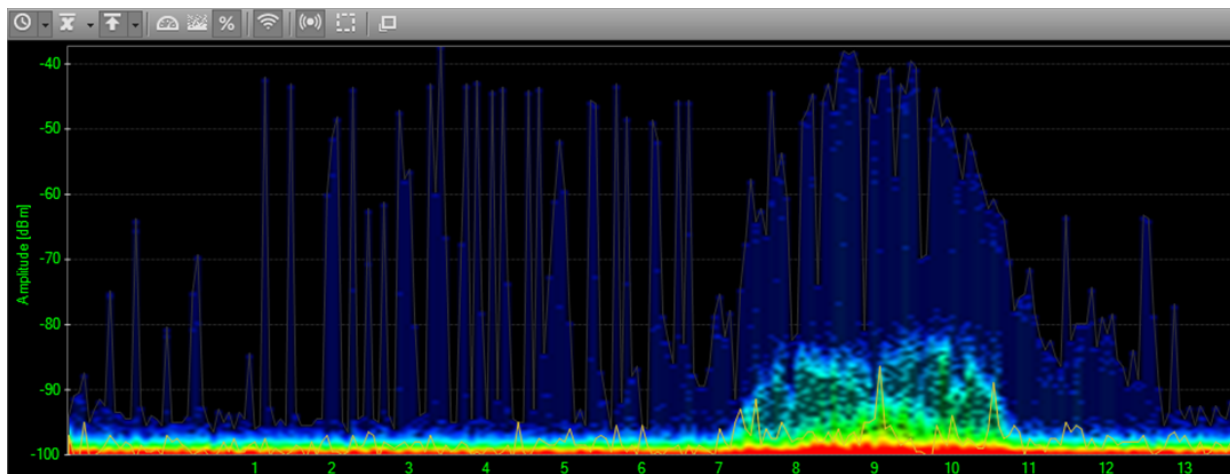
- **Coherent interference:** a result of another device using the same channel as your AP, or poor planning of a wireless infrastructure (perhaps the other nearby APs are using the same channel or the signal strength is too high).
- **Non-coherent interference:** a result of other radio signals such as bluetooth, microwave, cordless phone, or (as in medical environments) x-ray machines.

Most common and simple solution for frequency interference is to change your operation channel. Typically, the channel can be set from 1 to 11 for the broadcast frequency, although you should always use channels 1, 6, and 11 on the 2.4GHz band.

Another solution, if it's appropriate for your location, is to use the 5GHz band instead.

### MetaGeek Chanalyzer

You can perform a site survey using spectrum analysis at various points in your environment looking for signal versus interference/noise. MetaGeek Chanalyzer is an example of a third party utility which shows a noise threshold.



Note that a signal of -95dBm or less will be ignored by Fortinet wireless adapters.

## Throughput issues

Sometimes communication issues can be caused by low performance.

### Testing the link

You can identify delays or lost packets by sending ping packets from your wireless client. If there is more than 10ms of delay, there may be a problem with your wireless deployment, such as:

- a weak transmit signal from the client (the host does not reach the AP)
- the AP utilization is too high (your AP could be saturated with connected clients)
- interference (third party signal could degrade your AP or client's ability to detect signals between them)

- weak transmit power from the AP (the AP does not reach the host) -- not common in a properly deployed network, unless the client is too far away

Keep in mind that water will also cause a reduction in radio signal strength for those making use out of outdoor APs or wireless on a boat.

## Performance testing

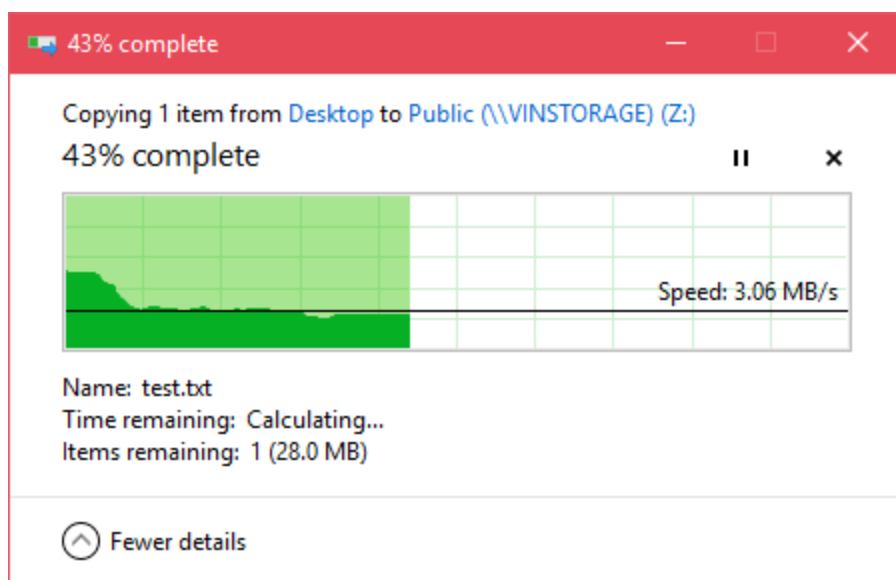
If the FortiAP gives bad throughput to the client, the link may drop. The throughput or performance can be measured on your smartphone with third party applications tool such as iPerf and jPerf.

### Measuring file transfer speed

Another way to get a sense of your throughput issues is to measure the speed of a file transfer on your network. Create a test file at a specific size and measure the speed at which Windows measures the transfer. The command below will create a 50MB file.

- `fsutil file createnew test.txt 52428800`

The following image shows a network transfer speed of just over 24Mbps. The theoretical speed of 802.11g is 54Mbps, which is what this client is using. A wireless client is never likely to see the theoretical speed.



### TKIP limitation

If you find that throughput is a problem, avoid WPA security encrypted with Temporal Key Integrity Protocol (TKIP) as it supports communications only at 54Mbps. Use WPA-2 AES instead.

Speeds are very much based on what the client computer can handle as well. The maximum client connection rate of 130Mbps is for 2.4GHz on a 2x2, or 300Mbps for 5Ghz on a 2x2 (using shortguard and channel bonding enabled).

If you want to get more than 54Mbps with 802.11n, do not use legacy TKIP, use CCMP instead. This is standard for legacy compatibility.

## Preventing IP fragmentation in CAPWAP

TKIP is not the only possible source of decreased throughput. When a wireless client sends jumbo frames using a CAPWAP tunnel, it can result in data loss, jitter, and decreased throughput.

Using the following commands you can customize the uplink rates and downlink rates in the CAPWAP tunnel to prevent fragmentation and avoid data loss.

```
config wireless-controller wtp
  edit new-wtp
    set override-ip-fragment enable
    set ip-fragment-preventing [tcp-mss-adjust | icmp-unreachable]
    set tun-mtu-uplink [0 | 576 | 1500]
    set tun-mtu-downlink [0 | 576 | 1500]
  end
end
```

The default value is 0, however the recommended value will depend on the type of traffic. For example, IPsec in tunnel mode has 52 bytes of overhead, so you might use 1400 or less for uplink and downlink.

## Slowness in the DTLS response

It's important to know all the elements involved in the CAPWAP association:

- Request
- Response
- DTLS
- Join
- Configuration

All of these are bidirectional. So if the DTLS response is slow, this might be the result of a configuration error. This issue can also be caused by a certificate during discovery response. You can read more about this in [RFC 5416](#).

## Connection issues

If the client has a connectivity issue that is not due to signal strength, the solution varies by the symptom.

### Client connection issues

1. If client is unable to connect to FortiAP:
  - Make sure the client's security and authentication settings match with FortiAP and check the certificates as well.
  - Try upgrading the Wi-Fi adapter driver and FortiGate/FortiAP firmware.
  - If other clients can connect, it could be interoperability; run debug commands and sniffer packets.
  - Look for rogue suppression by sniffing the wireless traffic and looking for the disconnect in the output (using the AP or wireless packet sniffer).
  - Try changing the IEEE protocol from 802.11n to 802.11bg or 802.11a only.



2. If the client drops and reconnects:
  - The client might be de-authenticating periodically. Check the sleep mode on the client.
  - The issue could be related to power-saver settings. The client may need to update drivers.
  - The issue could also be caused by flapping between APs. Check the roaming sensitivity settings on the client or the preferred wireless network settings on the client—if another WiFi network is available, the client may connect to it if it is a preferred network. Also, check the DHCP configuration as it may be an IP conflict.
3. If the client drops and never connects:
  - It could have roamed to another SSID, so check the standby and sleep modes.
  - You may need to bring the interface up and down.
4. If the client connects, but no IP address is acquired by the client:
  - Check the DHCP configuration and the network.
  - It could be a broadcast issue, so check the WEP encryption key and set a static IP address and VLANs.

## Debug

You should also enable client debug on the controller for problematic clients to see the stage at which the client fails to connect. Try to connect from the problematic client and run the following debug command, which allows you to see the four-way handshake of the client association:

```
diagnose wireless-controller wlac sta_filter <client MAC address> 2
```

### Example of a successful client connection:

The following is a sample debug output for the above command, with successful association/DHCP phases and PSK key exchange (identified in color):

```
FG600B3909600253 #
91155.197 <ih> IEEE 802.11 mgmt::assoc_req <== 30:46:9a:f9:fa:34 vap signal-check rId 0
wId 0 00:09:0f:f3:20:45
91155.197 <ih> IEEE 802.11 mgmt::assoc_resp ==> 30:46:9a:f9:fa:34 vap signal-check rId 0
wId 0 00:09:0f:f3:20:45 resp 0
91155.197 <cc> STA_CFG_REQ(15) sta 30:46:9a:f9:fa:34 add ==> ws (0-192.168.35.1:5246) rId 0
wId 0
91155.197 <dc> STA add 30:46:9a:f9:fa:34 vap signal-check ws (0-192.168.35.1:5246) rId 0
wId 0 bssid 00:09:0f:f3:20:45 NON-AUTH
91155.197 <cc> STA add 30:46:9a:f9:fa:34 vap signal-check ws (0-192.168.35.1:5246) rId 0
wId 0 00:09:0f:f3:20:45 sec WPA2 AUTO auth 0
91155.199 <cc> STA_CFG_RESP(15) 30:46:9a:f9:fa:34 <== ws (0-192.168.35.1:5246) rc 0
(Success)
91155.199 <eh> send 1/4 msg of 4-Way Handshake
91155.199 <eh> send IEEE 802.1X ver=1 type=3 (EAPOL_KEY) data len=95 replay cnt 1
91155.199 <eh> IEEE 802.1X (EAPOL 99B) ==> 30:46:9a:f9:fa:34 ws (0-192.168.35.1:5246) rId 0
wId 0 00:09:0f:f3:20:45
91155.217 <eh> IEEE 802.1X (EAPOL 121B) <== 30:46:9a:f9:fa:34 ws (0-192.168.35.1:5246) rId 0
wId 0 00:09:0f:f3:20:45
91155.217 <eh> recv IEEE 802.1X ver=1 type=3 (EAPOL_KEY) data len=117
91155.217 <eh> recv EAPOL-Key 2/4 Pairwise replay cnt 1
91155.218 <eh> send 3/4 msg of 4-Way Handshake
91155.218 <eh> send IEEE 802.1X ver=1 type=3 (EAPOL_KEY) data len=175 replay cnt 2
91155.218 <eh> IEEE 802.1X (EAPOL 179B) ==> 30:46:9a:f9:fa:34 ws (0-192.168.35.1:5246) rId 0
wId 0 00:09:0f:f3:20:45
91155.223 <eh> IEEE 802.1X (EAPOL 99B) <== 30:46:9a:f9:fa:34 ws (0-192.168.35.1:5246) rId 0
wId 0 00:09:0f:f3:20:45
91155.223 <eh> recv IEEE 802.1X ver=1 type=3 (EAPOL_KEY) data len=95
```

```

91155.223 <eh> recv EAPOL-Key 4/4 Pairwise replay cnt 2
91155.223 <dc> STA chg 30:46:9a:f9:fa:34 vap signal-check ws (0-192.168.35.1:5246) rId 0
wId 0 bssid 00:09:0f:f3:20:45 AUTH
91155.224 <cc> STA chg 30:46:9a:f9:fa:34 vap signal-check ws (0-192.168.35.1:5246) rId 0
wId 0 00:09:0f:f3:20:45 sec WPA2 AUTO auth 1
91155.224 <cc> STA_CFG_REQ(16) sta 30:46:9a:f9:fa:34 add key (len=16) ==> ws (0-
192.168.35.1:5246) rId 0 wId 0
91155.226 <cc> STA_CFG_RESP(16) 30:46:9a:f9:fa:34 <== ws (0-192.168.35.1:5246) rc 0
(Success)
91155.226 <eh> ***pairwise key handshake completed*** (RSN)
91155.257 <dc> DHCP Request server 0.0.0.0 <== host ADMINFO-FD4I2HK mac 30:46:9a:f9:fa:34
ip 172.16.1.16
91155.258 <dc> DHCP Ack server 172.16.1.1 ==> host mac 30:46:9a:f9:fa:34 ip 172.16.1.16
mask 255.255.255.0 gw 172.16.1.1

```

where:

- **orange** represents the association phase,
- **blue** represents the PSK exchange,
- and **green** represents the DHCP phase.

It is important to note the messages for a correct association phase, four-way handshake, and DHCP phase.

## Checking WiFi password

Admins can view plain text passwords (captive-portal-radius-secret and passphrase) under `config wireless-controller vap`.

Note that `security` must be set as a WPA-personal setting.

## FortiAP connection issues

Clients are not the only device that can fail to connect, of course. A communication problem could arise from the FortiAP.

Some examples include:

- The FortiAP is not connecting to the wireless controller.
- One FortiAP intermittently disconnects and re-connects.
- All FortiAPs intermittently disconnect and re-connect.
- Unable to Telnet to FortiAP from controller/administrator workstation.

In the above cases:

- Check networking on the distribution system for all related FortiAPs.
- Check the authorization status of managed APs from the wireless controller.
- Restart the `cw_acd` process (**Note:** All APs will drop if you do this, and you may be troubleshooting just one AP).
- Check the controller crash log for any wireless controller daemon crash using the following command:

```
diagnose debug crashlog read
```

## Debug

For a quick assessment of the association communication between the controller and the FortiAP, run the following sniffer command to see if you can verify that the AP is communicating to the controller by identifying the

## CAPWAP communication:

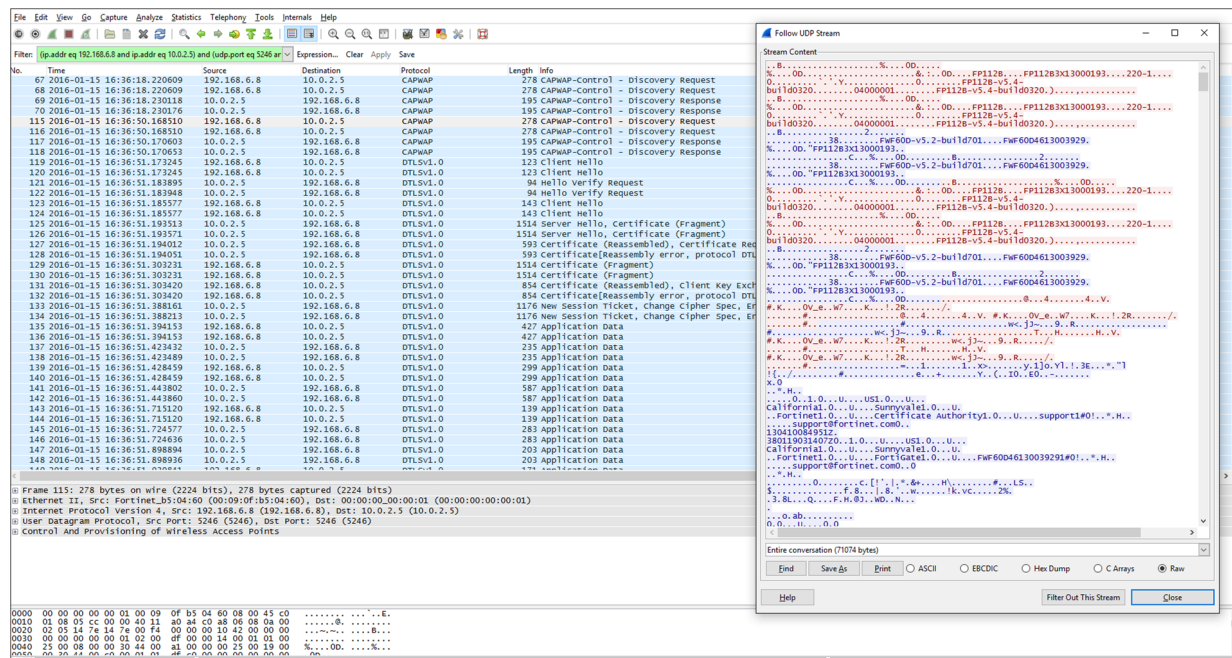
```
diagnose sniff packet <interface_name> "port 5246" 4
```

If you do not see this communication, then you can investigate the network or the settings on the AP to see why it is not reaching the controller.

The following command allows you to collect verbose output from the sniff that can be converted to a PCAP and viewed in Wireshark.

```
diagnose sniff packet <interface_name> "port 5246" 6 o 1
```

The image below shows the beginning of the AP's association to the controller. You can see the discovery Request and Response at the top.



Throughout debugging it is recommended to:

- Enable Telnet login to the FortiAP device so that you can log in and issue local debugging commands:

```
config wireless-controller wtp
edit "<FortiAP_serial_number>"
set override-allowaccess {disable|enable}
set allowaccess {telnet | http | https | ssh}
end
```

- Try to connect to the wireless controller from the problematic FortiAP to verify routes exist.
- Enable wtp (FortiAP) debugging on the wireless controller for problematic FortiAPs to determine the point at which the FortiAP fails to connect:

```
diag wireless-controller wlac wtp_filter FP112B3X13000193 0-192.168.6.8:5246 2
(replace the serial number and IP address of the FortiAP)
di de console timestamp en
di de application cw_acd 0x7ff
di de en
```

**Example of a successful AP and controller association:**

The previous debug command provides similar output to the sample debug message below for a successful association between the FortiAP and the wireless controller. This includes the elements of the CAPWAP protocol; the Request, Response, DTLS, Join, and Configuration (identified in color). All of these are bi-directional, so if the DTLS response is slow, it may be an example of a configuration error.

```

56704.575 <msg> DISCOVERY_REQ (12) <== ws (0-192.168.35.1:5246)
56704.575 <msg> DISCOVERY_RESP (12) ==> ws (0-192.168.35.1:5246)
56707.575 <msg> DISCOVERY_REQ (13) <== ws (0-192.168.35.1:5246)
56707.575 <msg> DISCOVERY_RESP (13) ==> ws (0-192.168.35.1:5246)
56709.577 <aev> - CWAE_INIT_COMPLETE ws (0-192.168.35.1:5246)
56709.577 <aev> - CWAE_LISTENER_THREAD_READY ws (0-192.168.35.1:5246)
56709.577 <fsm> old CWAS_START(0) ev CWAE_INIT_COMPLETE(0) new CWAS_IDLE(1)
56709.577 <fsm> old CWAS_IDLE(1) ev CWAE_LISTENER_THREAD_READY(1) new CWAS_DTLS_SETUP(4)
56709.623 <aev> - CWAE_DTLS_PEER_ID_RECV ws (0-192.168.35.1:5246)
56709.623 <aev> - CWAE_DTLS_AUTH_PASS ws (0-192.168.35.1:5246)
56709.623 <aev> - CWAE_DTLS_ESTABLISHED ws (0-192.168.35.1:5246)
56709.623 <fsm> old CWAS_DTLS_SETUP(4) ev CWAE_DTLS_PEER_ID_RECV(7) new CWAS_DTLS_
AUTHORIZE(2)
56709.623 <fsm> old CWAS_DTLS_AUTHORIZE(2) ev CWAE_DTLS_AUTH_PASS(3) new CWAS_DTLS_CONN(5)
56709.623 <fsm> old CWAS_DTLS_CONN(5) ev CWAE_DTLS_ESTABLISHED(8) new CWAS_JOIN(7)
56709.625 <msg> JOIN_REQ (14) <== ws (0-192.168.35.1:5246)
56709.625 <aev> - CWAE_JOIN_REQ_RECV ws (0-192.168.35.1:5246)
56709.626 <fsm> old CWAS_JOIN(7) ev CWAE_JOIN_REQ_RECV(12) new CWAS_JOIN(7)
56709.629 <msg> CFG_STATUS (15) <== ws (0-192.168.35.1:5246)
56709.629 <aev> - CWAE_CFG_STATUS_REQ ws (0-192.168.35.1:5246)
56709.629 <fsm> old CWAS_JOIN(7) ev CWAE_CFG_STATUS_REQ(13) new CWAS_CONFIG(8)
56710.178 <msg> CHG_STATE_EVENT_REQ (16) <== ws (0-192.168.35.1:5246)
56710.178 <aev> - CWAE_CHG_STATE_EVENT_REQ_RECV ws (0-192.168.35.1:5246)
56710.178 <fsm> old CWAS_CONFIG(8) ev CWAE_CHG_STATE_EVENT_REQ_RECV(23) new CWAS_DATA_
CHAN_SETUP(10)
56710.220 <aev> - CWAE_DATA_CHAN_CONNECTED ws (0-192.168.35.1:5246)
56710.220 <msg> DATA_CHAN_KEEP_ALIVE <== ws (0-192.168.35.1:5246)
56710.220 <aev> - CWAE_DATA_CHAN_KEEP_ALIVE_RECV ws (0-192.168.35.1:5246)
56710.220 <msg> DATA_CHAN_KEEP_ALIVE ==> ws (0-192.168.35.1:5246)
56710.220 <fsm> old CWAS_DATA_CHAN_SETUP(10) ev CWAE_DATA_CHAN_CONNECTED(32) new CWAS_
DATA_CHECK(11)
56710.220 <aev> - CWAE_DATA_CHAN_VERIFIED ws (0-192.168.35.1:5246)
56710.220 <fsm> old CWAS_DATA_CHECK(11) ev CWAE_DATA_CHAN_KEEP_ALIVE_RECV(35) new CWAS_
DATA_CHECK(11)
56710.220 <fsm> old CWAS_DATA_CHECK(11) ev CWAE_DATA_CHAN_VERIFIED(36) new CWAS_RUN(12)
56710.228 <msg> WTP_EVENT_REQ (17) <== ws (0-192.168.35.1:5246)
56710.228 <aev> - CWAE_WTP_EVENT_REQ_RECV ws (0-192.168.35.1:5246)
56710.228 <fsm> old CWAS_RUN(12) ev CWAE_WTP_EVENT_REQ_RECV(42) new CWAS_RUN(12)
56710.230 <msg> CFG_UPDATE_RESP (1) <== ws (0-192.168.35.1:5246) rc 0 (Success)
56710.230 <aev> - CWAE_CFG_UPDATE_RESP_RECV ws (0-192.168.35.1:5246)
56710.230 <msg> WTP_EVENT_REQ (18) <== ws (0-192.168.35.1:5246)
56710.230 <aev> - CWAE_WTP_EVENT_REQ_RECV ws (0-192.168.35.1:5246)
56710.230 <fsm> old CWAS_RUN(12) ev CWAE_CFG_UPDATE_RESP_RECV(37) new CWAS_RUN(12)
56710.230 <fsm> old CWAS_RUN(12) ev CWAE_WTP_EVENT_REQ_RECV(42) new CWAS_RUN(12)
56710.231 <msg> WTP_EVENT_REQ (19) <== ws (0-192.168.35.1:5246)
56710.231 <aev> - CWAE_WTP_EVENT_REQ_RECV ws (0-192.168.35.1:5246)
56710.231 <fsm> old CWAS_RUN(12) ev CWAE_WTP_EVENT_REQ_RECV(42) new CWAS_RUN(12)
56710.232 <msg> CFG_UPDATE_RESP (2) <== ws (0-192.168.35.1:5246) rc 0 (Success)
56710.232 <aev> - CWAE_CFG_UPDATE_RESP_RECV ws (0-192.168.35.1:5246)

```

```

56710.232 <fsm> old CWAS_RUN(12) ev CWAE_CFG_UPDATE_RESP_RECV(37) new CWAS_RUN(12)
56710.233 <msg> WTP_EVENT_REQ (20) <== ws (0-192.168.35.1:5246)
56710.233 <aev> - CWAE_WTP_EVENT_REQ_RECV ws (0-192.168.35.1:5246)
56710.233 <fsm> old CWAS_RUN(12) ev CWAE_WTP_EVENT_REQ_RECV(42) new CWAS_RUN(12)
56712.253 < . > AC (2) -> WTP (0-192.168.35.1:5246) State: CWAS_RUN (12) accept 3 live 3
           dbg 00000000 pkts 12493 0
56715.253 < . > AC (2) -> WTP (0-192.168.35.1:5246) State: CWAS_RUN (12) accept 3 live 6
           dbg 00000000 pkts 12493 0
56718.253 < . > AC (2) -> WTP (0-192.168.35.1:5246) State: CWAS_RUN (12) accept 3 live 9
           dbg 00000000 pkts 12493 0
56719.253 <aev> - CWAE_AC_ECHO_INTV_TMR_EXPIRE ws (0-192.168.35.1:5246)
56719.253 <fsm> old CWAS_RUN(12) ev CWAE_AC_ECHO_INTV_TMR_EXPIRE(39) new CWAS_RUN(12)
56719.576 <msg> ECHO_REQ (21) <== ws (0-192.168.35.1:5246)
56719.576 <aev> - CWAE_ECHO_REQ_RECV ws (0-192.168.35.1:5246)
56719.577 <fsm> old CWAS_RUN(12) ev CWAE_ECHO_REQ_RECV(27) new CWAS_RUN(12)

```

where:

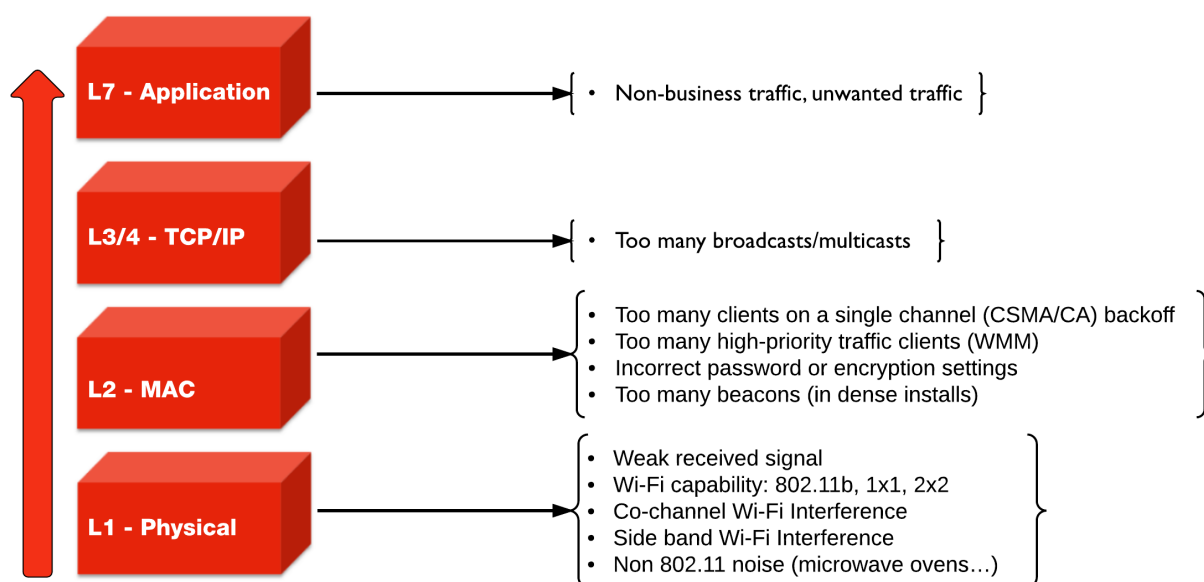
- **orange** represents the Discovery phase,
- **blue** indicates that the control channels have been established using DTLS,
- **green** represents the access point Discovery and Join phase,
- **purple** represents the Clear Text channel,
- and **pink** indicates that the FortiAP successfully connected to the wireless controller.

## General problems

Not all WiFi problems are related to signal strength, interference, or misconfiguration. The following OSI model identifies some of the more common issues per layer.

Best practices for troubleshooting vary depending on the affected layer (see below).

### Common sources of wireless issues



## Best practices for Layer 1

Common physical layer issues include:

- Weak received signal,
- WiFi capability: 802.11b, 1x1, 2x2,
- Co-channel WiFi interference,
- Side band WiFi interference,
- Non 802.11 noise (microwave ovens...).

To avoid physical layer issues:

- Determine RST (Receiver Sensitivity Threshold) for your device, or use -70dBm as a rule of thumb.
- Match AP TX output power to the client TX output power.
  - **Note:** iPhone TX power is only 10dBm.
- Use DFS (Dynamic Frequency Selection) for high performance data 20/40 MHz.
- Use 5GHz UNII-1 & 3 (Non-DFS) bands with static channel assignment for latency-sensitive applications.
- Do not use 40MHz channels in 2.4 GHz band (channel bonding is not allowed in FortiOS).

## Best practices for Layer 2

Common data link (MAC) layer issues include:

- Too many clients on a single channel (CSMA/CA) backoff,
- Too many high-priority traffic clients (WMM),
- Incorrect password or encryption settings,
- Too many beacons (in dense installs).

To avoid data link layer issues:

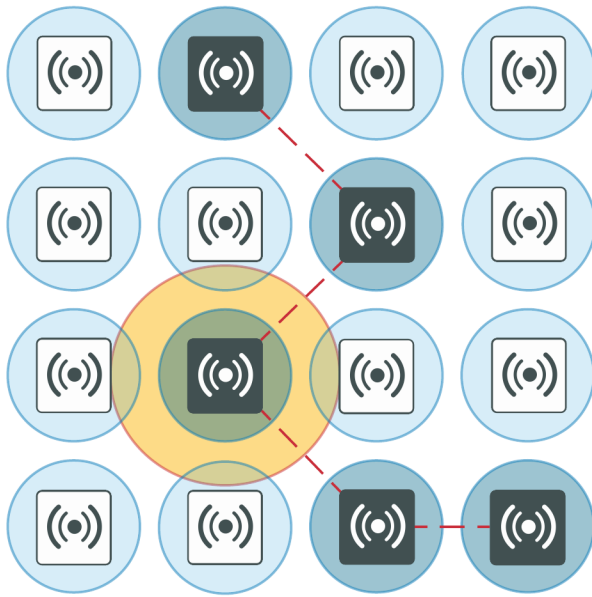
- Only use CCMP/AES (WPA2) encryption (not TKIP).
- In high density deployments, turn off SSID broadcast or turn down SSID rates. Review and possibly reduce the beacon interval.
- Determine the best cell size for applications:
  - For few users and low bandwidth latency sensitive applications, use high transmit power to create larger cells.
  - For high performance/high capacity installations, use lower transmit power to create smaller cells (set FortiPlanner at 10dBm TX power), but bear in mind that this will require more roaming.

## Cells and co-channel interference

In high density deployments, multiple APs are used, and each one services an area called a cell. However, these cells can cause interference with each other. This is a common problem. The radio signal from one AP interferes with, or cancels out, the radio signal from another AP.

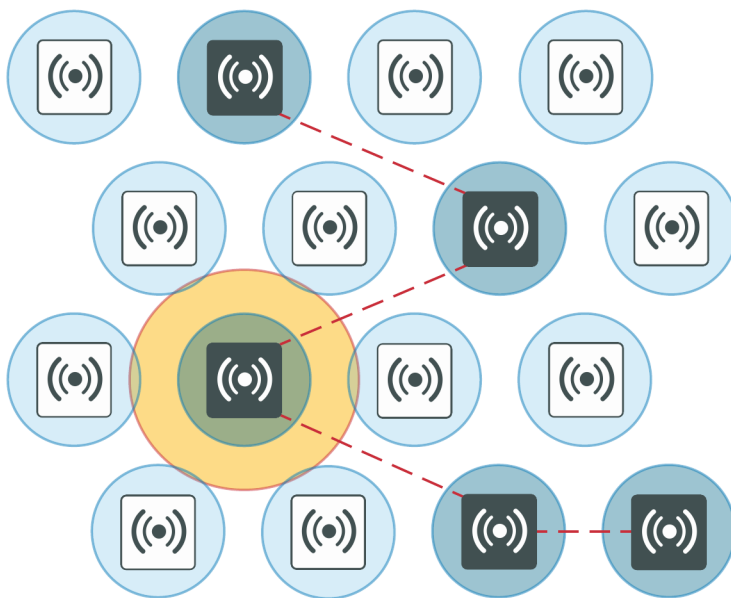
In the following diagram, note the interference zone created by one radio, causing interference on its neighbouring APs.

The interference zone can be twice the radius of the signal, and the signal at its edge can be -67dBm.



### Reducing co-channel interference

For best results, use a 'honeycomb' pattern as a deployment strategy. The idea is to *stagger* repeated channels furthest from each other to avoid interference.



### Best practices for Layer 3 and above

For TCP/IP layers and above, a common source of latency, or slowness in the wireless traffic, is too many broadcasts or multicasts. These types of issues can result from non-business and/or unwanted traffic.

To resolve issues at the TCP/IP layer and above:

- Identify business-critical applications.
- Use Application Control, Web Filtering, Traffic Shaping, and QoS to prioritize applications.
  - Identify unwanted traffic, high-bandwidth web-related traffic, and use Security Profiles.
  - Use the traffic shaper on a policy to rate-limit this traffic.

These configurations are performed directly on the FortiGate.

## Packet sniffer

Capturing the traffic between the controller and the FortiAP can help you identify most FortiAP and client connection issues.

This section describes the following recommended packet sniffing techniques:

- [CAPWAP packet sniffer](#)
- [Wireless traffic packet sniffer](#)

### CAPWAP packet sniffer

The first recommended technique consists of sniffing the CAPWAP traffic.

- Enable plain control on the controller and on the FortiAP to capture clear control traffic on UDP port 5246.

- On the controller:

```
diagnose wireless-controller wlac plain-ctl <FortiAP_serial_number> 1
```

**Result:**

```
WTP 0-FortiAP2223X11000107 Plain Control: enabled
```

- On the FortiAP:

```
cw_diag plain-ctl 1
```

**Result:**

```
Current Plain Control: enabled
```

Note that some issues are related to the keep-alive for control and data channel.

- Data traffic on UDP port 5247 is not encrypted. The data itself is encrypted by the wireless security mechanism.

Data traffic is helpful to troubleshoot most of the issues related to station association, EAP authentication, WPA key exchange, roaming, and FortiAP configuration.

You can also set up a host or server to which you can forward the CAPWAP traffic:

1. Configure the host/server to which CAPWAP traffic is forwarded:

```
diagnose wireless-controller wlac sniff-cfg <Host_IP_address> 88888
```

**Result:**

```
Current Sniff Server: 192.168.25.41, 23352
```

2. Choose which traffic to capture, the interface to which the FortiAP is connected, and the FortiAP's serial number:

```
diagnose wireless-controller wlac sniff <interface_name> <FortiAP_serial_number> 2
```

**Result:**



WTP 0-FortiAP2223X11000107 Sniff: intf port2 enabled (control and data message)

In the above syntax, the '2' captures the control and data message—'1' would capture only the control message, and '0' would disable it.

- Run Wireshark on the host/server to capture CAPWAP traffic from the controller.
  - Decode the traffic as IP to check inner CAPWAP traffic.

### Example CAPWAP packet capture

The following image shows an example of a CAPWAP packet capture, where you can see: the Layer 2 header; the sniffed traffic encapsulated into Internet Protocol for transport; CAPWAP encapsulated into UDP for sniffer purpose and encapsulated into IP; CAPWAP control traffic on UDP port 5246; and CAPWAP payload.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.35.82	192.168.35.80	CAPWAP	Control Msg - Echo Request
2	0.000308	192.168.35.82	192.168.35.80	CAPWAP	Control Msg - Echo Request
3	0.000452	192.168.35.80	192.168.35.82	CAPWAP	Control Msg - Echo Response
4	0.000454	192.168.35.80	192.168.35.82	CAPWAP	Control Msg - Echo Response

## Wireless traffic packet sniffer

The second recommended technique consists of sniffing the wireless traffic directly 'on the air' using your FortiAP.

### Wireless traffic packet capture

Packet captures are useful for troubleshooting all wireless client related issues because you can verify data rate and 802.11 parameters, such as radio capabilities, and determine issues with wireless signal strength, interference, or congestion on the network.

A radio can only capture one frequency at a time; one of the radios is set to sniffer mode depending on the traffic or channel required. You must use two FortiAPs to capture both frequencies at the same time.

- Set a radio on the FortiAP to monitor mode.

```
iwconfig wlan10
```

**Result:**

```
wlan10 IEEE 802.11na    ESSID:""
Mode:Monitor Frequency:5.18 GHz Access Point: Not-Associated
```

- The capture file is stored under the temp directory as *wl\_sniff.pcap*  
*/tmp/wl\_sniff.pcap*
  - Remember that the capture file is only stored temporarily. If you want to save it, upload it to a TFTP server before rebooting or changing the radio settings.
  - The command `cp wl_sniff.pcap newname.pcap` allows you to rename the file.
  - Rather than TFTP the file, you can also log in to the AP and retrieve the file via the web interface. Move the file using the command: `mv name /usr/www`

You can verify the file was moved using the command `cd /usr/www` and then browsing to: `<fortiAP_IP>/filename`

**Syntax**

The following syntax demonstrates how to set the radio to sniffer mode (configurable from the CLI only). Sniffer mode provides options to filter for specific traffic to capture. Notice that you can determine the buffer size, which channel to sniff, the AP's MAC address, and select if you want to sniff the beacons, probes, controls, and data channels.

```
configure wireless-controller wtp-profile
  edit <profile_name>
    configure <radio>
      set mode sniffer
      set ap-sniffer-bufsize 32
      set ap-sniffer-chan 1
      set ap-sniffer-addr 00:00:00:00:00:00
      set ap-sniffer-mgmt-beacon enable
      set ap-sniffer-mgmt-probe enable
      set ap-sniffer-mgmt-other enable
      set ap-sniffer-ctl enable
      set ap-sniffer-data enable
    end
  end
```

Once you've performed the previous CLI configuration, you'll be able to see the packet sniffer mode selected in the GUI dashboard under **WiFi & Switch Controller > FortiAP Profiles** and **WiFi & Switch Controller > Managed FortiAPs**. Bear in mind that if you change the mode from the GUI, you'll have to return to the CLI to re-enable the Sniffer mode.

To disable the sniffer profile in the CLI, use the following commands:

```
config wireless-controller wtp-profile
  edit <profile_name>
    config <radio>
      set ap-sniffer-mgmt-beacon disable
      set ap-sniffer-mgmt-probe disable
      set ap-sniffer-mgmt-other disable
      set ap-sniffer-ctl disable
      set ap-sniffer-data disable
    end
```

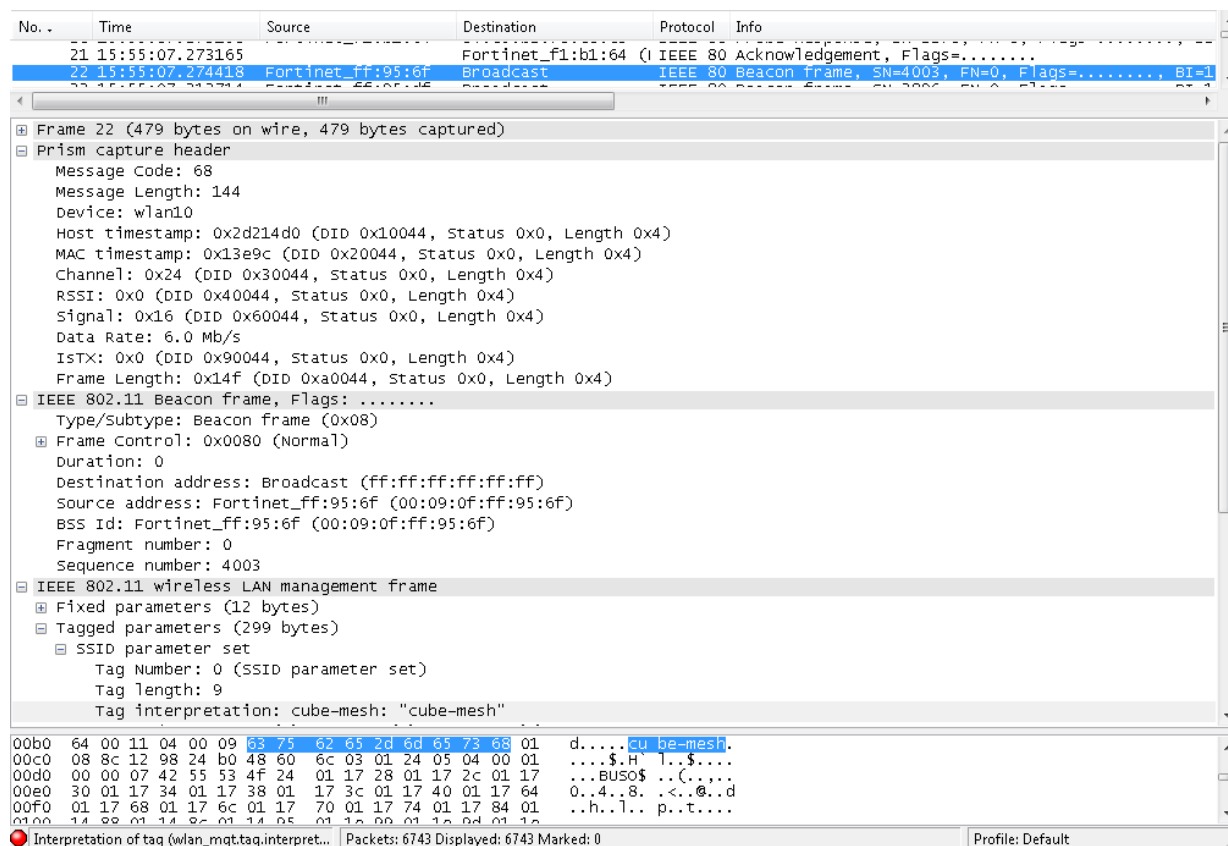
end



If you change the radio mode before sending the file *wl\_sniff.cap* to an external TFTP, the file will be deleted and you will lose your packet capture.

### Example AP packet capture

The following image shows an example of the AP packet capture. Note the capture header showing channel 36; the beacon frame; the source, destination, and BSSID of the beacon frame; and the SSID of the beacon frame.



## Useful debugging commands

For a comprehensive list of useful debug options you can use the following help commands on the controller:

```
diagnose wireless-controller wlac help
(this command lists the options available that pertain to the wireless controller)
```

```
diagnose wireless-controller wlwt help
(this command lists the options available that pertain to the AP)
```

## Sample outputs

### Syntax

```
diagnose wireless-controller wlac -c vap
```

(this command lists the information about the virtual access point, including its MAC address, the BSSID, its SSID, the interface name, and the IP address of the APs that are broadcasting it)

#### Result:

bssid	ssid	intf	vfid:ip-port	rId	wId
00:09:0f:d6:cb:12	Office	Office	ws (0-192.168.3.33:5246)	0	0
00:09:0f:e6:6b:12	Office	Office	ws (0-192.168.1.61:5246)	0	0
06:0e:8e:27:dc:48	Office	Office	ws (0-192.168.3.36:5246)	0	0
0a:09:0f:d6:cb:12	public	publicAP	ws (0-192.168.3.33:5246)	0	1

### Syntax

```
diagnose wireless-controller wlac -c darrp
```

(this command lists the information pertaining to the radio resource provisioning statistics, including the AP serial number, the number of channels set to choose from, and the operation channel. Note that the 5GHz band is not available on these APs listed)

#### Result:

wtp_id	rId	base_mac	index	nr_chan	vfid	5G	oper_chan	age
FAP22A3U10600400	0	00:09:0f:d6:cb:12	0	3	0	No	1	87588
FW80CM3910601176	0	06:0e:8e:27:dc:48	1	3	0	No	6	822

## Support for extension information for wtp, vap, and station

You can enable or disable extension information at `wtp-profile`, and use the diagnose option below to print out the detail of extension information.

### Syntax

```
config wireless-controller wtp-profile
edit test
    set lldp [enable | disable]
    set ext-info [enable | disable] --> Enable/disable station/VAP/radio extension information.
end
end

diagnose wireless-controller wlac -d [wtp | vap | sta]
```

where:

- `wlac -d wtp [SN|name] [reset]` --> list or reset wtp info(data)
- `wlac -d vap [bssid] [reset]` --> list or reset vap info(data)
- `wlac -d sta [mac] [reset]` --> list or reset sta info(data)

# Reference

This chapter provides some reference information pertaining to wireless networks.

[FortiAP web-based manager](#)

[Wireless radio channels](#)

[WiFi event types](#)

[FortiAP CLI](#)

## FortiAP web-based manager

You can access the FortiAP unit's built-in web-based manager. This is useful to adjust settings that are not available through the FortiGate unit's WiFi Controller. Logging into the FortiAP web-based manager is similar to logging into the FortiGate web-based manager.

### System information

#### Status

The **Status** section provides information about the FortiAP unit.

Host Name	FAP22B3U11005354 <a href="#">[Change]</a>
Serial Number	FAP22B3U11005354
Region Code	A
Firmware Version	FortiAP-220B v5.0,build064,140117 (GA) <a href="#">[Update]</a>
Network Status	0.0.0.0/0.0.0.0/0.0.0.0 (Mon Jun 2 12:50:05 2014)
System Time	Tue May 27 13:00:39 2014
Current Administrator	admin <a href="#">[Change Password]</a>
System Configuration	Last Backup: N/A <a href="#">[Backup]</a> <a href="#">[Restore]</a>
Uptime	7 day(s) 2 hour(s) 4 min(s)
CPU Usage	<div><div></div></div> 1%
Memory Usage	<div><div></div></div> 35%
AC Discovery Status	Discovering AC ...

You can:

- Select **Change** to change the **Host Name**.
- Select **Update** in **Firmware Version** to upload a new FortiAP firmware file from your computer.
- Select **Change Password** to change the administrator password.
- Select **Backup** to save the current FortiAP configuration as a file on your computer.
- Select **Restore** to load a configuration into your FortiAP unit from a file on your computer.

#### Network configuration

Select DHCP or select Static and specify the IP address, netmask, and gateway IP address. **Administrative Access** settings affect access after the FortiAP has been authorized. By default, **HTTP** access needed to access the FortiAP web-based manager is enabled, but **Telnet** access is not enabled.

#### Connectivity

These settings determine how the FortiAP unit connects to the FortiGate WiFi controller.

<b>Uplink</b>	Ethernet - wired connection to the FortiGate unit (default)  Mesh - WiFi mesh connection  Ethernet with mesh backup support
<b>Mesh AP SSID</b>	Enter the SSID of the mesh root. Default: fortinet.mesh.root
<b>Mesh AP Password</b>	Enter password for the mesh SSID.
<b>Ethernet Bridge</b>	Bridge the mesh SSID to the FortiAP Ethernet port.  This is available only when <b>Uplink</b> is <b>Mesh</b> .

## WTP configuration

AC Discovery Type settings affect how the FortiAP unit discovers a FortiGate WiFi controller. By default, this is set to Auto which causes the FortiAP unit to cycle through all of the discovery methods until successful. For more information see Controller discovery methods.

<b>AC Discovery Type</b>	Static, DHCP, DNS, Broadcast, Multicast, Auto
<b>AC Control Port</b>	Default port is 5246.
<b>AC IP Address 1</b> <b>AC IP Address 2</b> <b>AC IP Address 3</b>	You enter up to three WiFi controller IP addresses for static discovery. Routing must be properly configured in both directions.
<b>AC Host Name 1</b> <b>AC Host Name 2</b> <b>AC Host Name 3</b>	As an alternative to AC IP addresses, you can enter their fully qualified domain names (FQDNs).
<b>AC Discovery Multicast Address</b>	224.0.1.140
<b>AC Discovery DHCP Option Code</b>	When using DHCP discovery, you can configure the DHCP server to provide the controller address. By default the FortiAP unit expects this in option 138.

**AC Data Channel Security** by default accepts either DTLS-encrypted or clear text data communication with the WiFi controller. You can change this setting to require encryption or to use clear text only.

## Wireless information

The Wireless Information page provides current information about the operation of the radios and the type Uplink in use.

## Wireless radio channels

### IEEE 802.11a/n channels

The following table lists the channels supported on FortiWiFi products that support the IEEE 802.11a and 802.11n wireless standards. 802.11a is available on FortiWiFi models 60B and higher. 802.11n is available on FortiWiFi models 80CM and higher.

All channels are restricted to indoor usage except in the Americas, where both indoor and outdoor use is permitted on channels 52 through 64 in the United States.

#### IEEE 802.11a/n (5-GHz Band) channel numbers

Channel number	Frequency (MHz)	Regulatory Areas				
		Americas	Europe	Taiwan	Singapore	Japan
34	5170					•
36	5180	•	•		•	
38	5190					
40	5200	•	•		•	•
42	5210					
44	5220	•	•		•	•
46	5230					
48	5240	•	•		•	•
149	5745	•		•	•	
153	5765	•		•	•	
157	5785	•		•	•	
161	5805	•		•	•	
165	5825	•			•	

#### IEEE 802.11b/g/n channel numbers

The following table lists IEEE 802.11b/g/n channels. All FortiWiFi units support 802.11b and 802.11g. Newer models also support 802.11n.



Mexico is included in the Americas regulatory domain. Channels 1 through 8 are for indoor use only. Channels 9 through 11 can be used indoors and outdoors. You must make sure that the channel number complies with the regulatory standards of Mexico.

### IEEE 802.11b/g/n (2.4-GHz Band) channel numbers

Channel number	Frequency (MHz)	Regulatory Areas			
		Americas	EMEA	Israel	Japan
1	2412	•	•	indoor	•
2	2417	•	•	indoor	•
3	2422	•	•	indoor	•
4	2427	•	•	indoor	•
5	2432	•	•	•	•
6	2437	•	•	•	•
7	2442	•	•	•	•
8	2447	•	•	•	•
9	2452	•	•	•	•
10	2457	•	•	•	•
11	2462	•	•	•	•
12	2467		•	•	•
13	2472		•	•	•
14	2484				b only

### View all country and regcodes/regulatory domains

The following CLI command can be entered to view a list of the country and regcodes/regulatory Domains supported by Fortinet:

```
cw_diag -c all-countries
```

Below is a table showing a sample of the list displayed by entering this command:

Country-code	Region-code	Domain	ISO-name	Name
0	A	FCC3 & FCCA	NA	NO_COUNTRY_SET

Country-code	Region-code	Domain	ISO-name	Name
8	W	NULL1 & WORLD	AL	ALBANIA
12	W	NULL1 & WORLD	DZ	ALGERIA
16	A	FCC3 & FCCA	AS	AMERICAN SAMOA
...	...	...	...	...

## WiFi event types

Event type	Description
rogue-ap-detected	A rogue AP has been detected (generic).
rogue-ap-off-air	A rogue AP is no longer detected on the RF side.
rogue-ap-on-wire	A rogue AP has been detected on wire side (connected to AP or controller L2 network).
rogue-ap-off-wire	A rogue AP is no longer detected on wire.
rogue-ap-on-air	A rogue AP has been detected on the RF side.
fake-ap-detected	A rogue AP broadcasting on the same SSIDs that you have in your managed APs has been detected.
fake-ap-on-air	The above fake AP was detected on the RF side.

## FortiAP CLI

The FortiAP CLI controls radio and network operation through the use of variables manipulated with the `cfg` command. There are also diagnostic commands.

The `cfg` command include the following

<code>cfg -s</code>	List variables.
<code>cfg -a var=value</code>	Add or change a variable value.
<code>cfg -c</code>	Commit the change to flash.
<code>cfg -x</code>	Reset settings to factory defaults.

<code>cfg -r var</code>	Remove variable.
<code>cfg -e</code>	Export variables.
<code>cfg -h</code>	Display help for all commands.

The configuration variables are:

Var	Description and Values
AC_CTL_PORT	WiFi Controller control (CAPWAP) port. Default 5246.
AC_DATA_CHAN_SEC	Data channel security. 0 - Clear text 1 - DTLS (encrypted) 2 - Accept either DTLS or clear text (default)
AC_DISCOVERY_TYPE	1 - Static. Specify WiFi Controllers 2 - DHCP 3 - DNS 5 - Broadcast 6 - Multicast 0 - Cycle through all of the discovery types until successful.
AP_IPADDR AP_NETMASK IPGW	These variables set the FortiAP unit IP address, netmask and default gateway when ADDR_MODE is STATIC. Default 192.168.1.2 255.255.255.0, gateway 192.168.1.1.
AC_HOSTNAME_1 AC_HOSTNAME_2 AC_HOSTNAME_3	WiFi Controller host names for static discovery.
AC_IPADDR_1 AC_IPADDR_2 AC_IPADDR_3	WiFi Controller IP addresses for static discovery.
AC_DISCOVERY_DHCP_OPTION_CODE	Option code for DHCP server. Default 138.
AC_DISCOVERY_MC_ADDR	Multicast address for controller discovery. Default 224.0.1.140.

Var	Description and Values
ADDR_MODE	How the FortiAP unit obtains its IP address and netmask.  DHCP - FortiGate interface assigns address.  STATIC - Specify in AP_IPADDR and AP_NETMASK.  Default is DHCP.
ADMIN_TIMEOUT	Administrative timeout in minutes. Applies to Telnet and web-based manager sessions. Default is 5 minutes.
AP_MGMT_VLAN_ID	Non-zero value applies VLAN ID for unit management. Default: 0.
AP_MODE	FortiAP operating mode.  0 - Thin AP (default)  2 - Unmanaged Site Survey mode. See SURVEY variables.
BAUD_RATE	Console data rate: 9600, 19200, 38400, 57600, or 115200 baud.
DNS_SERVER	DNS Server for clients. If ADDR_MODE is DHCP the DNS server is automatically assigned.
FIRMWARE_UPGRADE	Default is 0.
HTTP_ALLOW	Access to FortiAP web-based manager 1 - Yes (default), 0 - No.
LED_STATE	Enable/disable status LEDs. 0 - LEDs enabled, 1 - LEDs disabled, 2 - follow AC setting.
LOGIN_PASSWD	Administrator login password. By default this is empty.
STP_MODE	Spanning Tree Protocol. 0 is off. 1 is on.
TELNET_ALLOW	By default (value 0), Telnet access is closed when the FortiAP unit is authorized. Set value to 1 to keep Telnet always available.
WTP_LOCATION	Optional string describing AP location.
<b>Mesh variables</b>	

Var	Description and Values
MESH_AP_BGSCAN	Enable or disable background mesh root AP scan. 0 - Disabled 1 - Enabled
MESH_AP_BGSCAN_RSSI	If the root AP's signal is weak, and lower than the received signal strength indicator (RSSI) threshold, the WiFi driver will immediately start a new round scan and ignore the configured MESH_AP_BGSCAN_PERIOD delays. Set the value between 0-127.  After the new round scan is finished, a scan done event is passed to wtp daemon to trigger roaming.
MESH_AP_BGSCAN_PERIOD	Time in seconds that a delay period occurs between scans. Set the value between 1-3600.
MESH_AP_BGSCAN_IDLE	Time in milliseconds. Set the value between 0-1000.
MESH_AP_BGSCAN_INTV	Time in milliseconds between channel scans. Set the value between 200-16000.
MESH_AP_BGSCAN_DUR	Time in milliseconds that the radio will continue scanning the channel. Set the value between 10-200.
MESH_AP_SCANCHANLIST	Specify those channels to be scanned.
MESH_AP_TYPE	Type of communication for backhaul to controller: 0 - Ethernet (default) 1 - WiFi mesh 2 - Ethernet with mesh backup support
MESH_AP_SSID	SSID for mesh backhaul. Default: fortinet.mesh.root
MESH_AP_BSSID	WiFi MAC address
MESH_AP_PASSWD	Pre-shared key for mesh backhaul.
MESH_ETH_BRIDGE	1 - Bridge mesh WiFi SSID to FortiAP Ethernet port. This can be used for point-to-point bridge configuration. This is available only when MESH_AP_TYPE =1.  0 - No WiFi-Ethernet bridge (default).

Var	Description and Values
MESH_MAX_HOPS	Maximum number of times packets can be passed from node to node on the mesh. Default is 4.
The following factors are summed and the FortiAP associates with the lowest scoring mesh AP.	
MESH_SCORE_HOP_WEIGHT	Multiplier for number of mesh hops from root. Default 50.
MESH_SCORE_CHAN_WEIGHT	AP total RSSI multiplier. Default 1.
MESH_SCORE_RATE_WEIGHT	Beacon data rate multiplier. Default 1.
MESH_SCORE_BAND_WEIGHT	Band weight (0 for 2.4GHz, 1 for 5GHz) multiplier. Default 100.
MESH_SCORE_RSSI_WEIGHT	AP channel RSSI multiplier. Default 100.
<b>Survey variables</b>	
SURVEY_SSID	SSID to broadcast in site survey mode (AP_MODE=2).
SURVEY_TX_POWER	Transmitter power in site survey mode (AP_MODE=2).
SURVEY_CH_24	Site survey transmit channel for the 2.4Ghz band (default 6).
SURVEY_CH_50	Site survey transmit channel for the 5Ghz band (default 36).
SURVEY_BEACON_INTV	Site survey beacon interval. Default 100msec.



Previously, FortiAP accepted Telnet and HTTP connection to any virtual interfaces that have an IP address. For security reasons, Telnet and HTTP access are now limited to br0 or br.vlan for AP\_MGMT\_VLAN\_ID.

Diagnose commands include:

<code>cw_diag help</code>	Display help for all diagnose commands.
<code>cw_diag uptime</code>	Show daemon uptime.
<code>cw_diag --tlog &lt;on off&gt;</code>	Turn on/off telnet log message.
<code>cw_diag --clog &lt;on off&gt;</code>	Turn on/off console log message.
<code>cw_diag baudrate [9600   19200   38400   57600   115200]</code>	Set the console baud rate.

<code>cw_diag plain-ctl [0 1]</code>	Show or change current plain control setting.
<code>cw_diag sniff-cfg ip port</code>	Set sniff server ip and port.
<code>cw_diag sniff [0 1 2]</code>	Enable/disable sniff packet.
<code>cw_diag stats wl_intf</code>	Show wl_intf status.
<code>cw_diag admin-timeout [30]</code>	Set shell idle timeout in minutes.
<code>cw_diag -c wtp-cfg</code>	Show current wtp config parameters in control plane.
<code>cw_diag -c radio-cfg</code>	Show current radio config parameters in control plane.
<code>cw_diag -c vap-cfg</code>	Show current vaps in control plane.
<code>cw_diag -c ap-rogue</code>	Show rogue APs pushed by AC for on-wire scan.
<code>cw_diag -c sta-rogue</code>	Show rogue STAs pushed by AC for on-wire scan.
<code>cw_diag -c arp-req</code>	Show scanned arp requests.
<code>cw_diag -c ap-scan</code>	Show scanned APs.
<code>cw_diag -c sta-scan</code>	Show scanned STAs.
<code>cw_diag -c sta-cap</code>	Show scanned STA capabilities.
<code>cw_diag -c wids</code>	Show scanned WIDS detections.
<code>cw_diag -c darrp</code>	Show darrp radio channel.
<code>cw_diag -c mesh</code>	Show mesh status.
<code>cw_diag -c mesh-veth-acinfo</code>	Show mesh veth ac info, and mesh ether type.
<code>cw_diag -c mesh-veth-vap</code>	Show mesh veth vap.
<code>cw_diag -c mesh-veth-host</code>	Show mesh veth host.
<code>cw_diag -c mesh-ap</code>	Show mesh ap candidates.
<code>cw_diag -c scan-clr-all</code>	Flush all scanned AP/STA/ARPs.
<code>cw_diag -c ap-suppress</code>	Show suppressed APs.
<code>cw_diag -c sta-deauth</code>	De-authenticate an STA.



Link aggregation can also be set in the CLI. Link aggregation is used to combine multiple network connections in parallel in order to increase throughput beyond what a single connection could sustain.

- FortiAP 320B and 320C models are supported.
- FortiAP 112B and 112D models **cannot** support link aggregation.
- NPI FAP-S3xxCR and "wave2" FAP/FAP-S models will have link aggregation feature via synchronization with regular FortiAP trunk build.





**FORTINET®**



Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.